2013-14 ANNUAL REPORT

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta
410, 9925 - 109 Street, NW
Edmonton, AB T5K 2J8

NOVEMBER 2014

Phone: 780.422.6860
Toll Free: 1.888.878.4044
Fax: 780.422.5682
Email: generalinfo@oipc.ab.ca

www.oipc.ab.ca

Office of the Information and
Privacy Commissioner of Alberta

November 2014

The Honourable Gene Zwozdesky
Speaker of the Legislative Assembly
325 Legislature Building
10800 - 97 Avenue
Edmonton, AB T5K 2B6

Dear Mr. Speaker:

I am honoured to present to the Legislative Assembly the Annual Report of the Office of the Information and Privacy Commissioner for the period April 1, 2013 to March 31, 2014.

This report is provided in accordance with section 63(1) of the *Freedom of Information and Protection of Privacy Act*, section 95(1) of the *Health Information Act*, and section 44(1) of the *Personal Information Protection Act*.

Yours truly,

Original signed by
Jill Clayton
Information and Privacy Commissioner

Table of Contents

Commissioner's Message 6

About the Office 9
Mandate 10
OIPC Organizational Structure 2013-14 12
The Process: Request for Review/Complaint 13
OIPC as a Public Body 14
Financial Overview 15

Trends and Issues 17
Emergencies and Disasters 18
Information Sharing 19
Focus on Access 20
Legislative Reform 21

By the Numbers 23
Statistics Reported by OIPC 25
Table 1: Cases Opened by Case Type 26
Table 2: Cases Closed by Case Type 27
Graph A: Total Cases Opened 28
Graph B: Total Cases Closed 28
Table 3: Percentage of Cases Closed by Resolution Method 29
Graph C: Percentage of Cases Closed by Resolution Method 29
Table 4: Telephone Calls, Emails And Written Enquiries 2013-14 30

Regulation and Enforcement 31
Request for Time Extensions Under FOIP 32
Mandatory Breach Reporting Under PIPA 33
Privacy Breach Reporting Under FOIP and HIA 34
Offence Investigations 35
Privacy Impact Assessment Reviews 35
Investigation Reports 36
Summary of Significant Decisions 39
Judicial Reviews and Other Court Decisions 42

Education and Outreach 49
Presentations, Forums and Workshops 50
Collaboration with Other Jurisdictions 52
Media Enquiries 53
Robert C. Clark Award 53

Financial Statements 55

Appendices 67
Appendix A: Cases Opened Under FOIP, HIA, PIPA by Entity Type 68
Appendix B: Cases Closed Under FOIP, HIA, PIPA by Entity Type 71
Appendix C: Orders, Decisions and Public Investigation Reports Issued 74
Appendix D: Accepted Privacy Impact Assessments by Public Body and Custodian Types 77

Commissioner's Message

Last December, Dictionary.com declared "privacy" its Word of the Year for 2013. Why? In an article on its website that referenced Edward Snowden, global spying, Project PRISM, airport body scanners, social media, Google, Apple, Facebook, Microsoft, Yahoo! and more, Dictionary.com concluded that "The discussion of privacy – what it is and what it isn't – embodies the preeminent concerns of [the year]."

In Canada, some of the most discussed issues of 2013-14 had privacy at their core, including the country's participation in global spying activities and the role of police, security and oversight agencies, as well as the introduction and debate of Bill C-13 to combat cyberbullying.

Privacy was also a leading topic in Alberta in 2013-14. Authorized users of health information systems were found snooping. A stolen unencrypted laptop containing health information of 631,000 Albertans in September 2013 resulted in one of the largest privacy breaches in Canada. Information sharing across public, private and health sectors continues with the increased focus on multi-agency citizen-centred service delivery.

Dictionary.com's choice of "privacy" as its Word of the Year is understandable. But I believe "transparency" could have also been a conceivable candidate.

Federally, we saw thwarted efforts to introduce sunshine laws to disclose the salaries of Members of Parliament, frustrated calls to modernize and renovate Canada's 30-year old access-to-information law, and extensive media coverage of Senate expenses. The public called for transparency as a means to achieve accountable government.

In Alberta, initial steps were taken towards increased openness with the launch of the government's Open Data portal and the proactive disclosure of salary and compensation information for certain employees, as well as the continued disclosure of the expenses of senior provincial government officials. Public bodies say they are receiving a greater number of FOIP requests and requests that are broader in scope. The OIPC has seen a 125% increase in time extension requests since 2011-12. At the same time, it appears public bodies increasingly refused to grant fee waivers, resulting in a 1,000% increase in requests to the OIPC to review these decisions since 2012-13.

In a year where privacy and access to information issues dominated public discourse, the Supreme Court of Canada struck down Alberta's *Personal Information Protection Act*, giving the Alberta Legislature 12 months to amend the Act's constitutional infirmity. Despite this result, the Court nevertheless emphasized the importance of privacy legislation, stating in its decision:

> The ability of individuals to control their personal information is intimately connected to their individual **autonomy, dignity and privacy**. These are **fundamental values that lie at the heart of a democracy**...legislation which aims to protect control over personal information should be characterized as **"quasi-constitutional"** because of the **fundamental role privacy plays in the preservation of a free and democratic society**... [emphasis added][1]

As much as privacy laws are fundamental to the preservation of a free and democratic society, access to information laws are similarly vital: as the means by which governments are held accountable to the citizenry. Both privacy and access laws are the cornerstone of democracy.

I urge the Government of Alberta to remember this as it concludes its review of the *Freedom of Information and Protection of Privacy Act* (the FOIP Act).

For a government that is under pressure to respond to an increasing number of access requests, the temptation may be to amend the legislation to restrict its scope, add exceptions to access, and increase fees so as to keep more information secret, away from the spotlight of the media, opposition and the public; to pay lip service to transparency and accountability, while diluting the legislation to ensure only innocuous information is ever disclosed. This approach, however, would only serve to underscore the perception of a government with something to hide.

Instead, now is the time to modernize and update the legislation to make it stronger, to rise above the day to day challenges and frustrations of implementing the law and to recognize that the strength of access-to-information legislation, and government's commitment to implementing it, is a direct reflection of the value government attributes to an informed citizenry and public debate - in a nutshell, the value government attributes to democracy itself.

Finally, as we carry on through 2014-15, I would like to take the opportunity to thank my colleagues at the OIPC for their grace, good humour and patience through recent changes in the office. Fiscal year 2013-14 was very much a time of transition as we implemented a new office structure and worked to consolidate our processes to establish a foundation for improved efficiency and effectiveness.

Jill Clayton
Information and Privacy Commissioner

[1] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733 at p. 747.

About the Office

Mandate

The Information and Privacy Commissioner is an Officer of the Legislature. The Commissioner reports directly to the Legislative Assembly of Alberta and is independent of the government of the day.

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in Alberta's three access and privacy Acts.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIP or the FOIP Act) applies to 1,160 public bodies, including provincial government departments and agencies, boards and commissions, municipalities, Métis settlements, drainage districts, irrigation districts, housing management bodies, school boards, post-secondary institutions, public libraries, police services, police commissions and health authorities.

The FOIP Act provides a right of access to any record in the custody or under the control of a public body, subject to limited and specific exceptions. The Act also gives individuals the right to access their own personal information held by public bodies and to request corrections to their own personal information. The Act protects privacy by setting out the circumstances in which a public body may collect, use, or disclose personal information.

Health Information Act

The *Health Information Act* (HIA) applies to more than 54,900 health custodians, including Alberta Health, Alberta Health Services, Covenant Health, nursing homes, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists, and dental hygienists.

HIA also applies to "affiliates," who perform a service for custodians, such as employees, contractors, students and volunteers. Custodians are responsible for the health information collected, used or disclosed by their affiliates.

HIA allows health services providers to exchange health information to provide care and to manage the health system.

The Act protects patients' privacy by regulating how health information may be collected, used and disclosed and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the right to access their own health information, to request corrections, and to have custodians consider their wishes regarding how much of their health information is disclosed or made accessible through Alberta's provincial electronic health record system (i.e. Alberta Netcare).

Personal Information Protection Act

The *Personal Information Protection Act* (PIPA) applies to provincially regulated private sector organizations, including businesses, corporations, associations, trade unions, private schools, private colleges, partnerships, professional regulatory organizations, and any individual acting in a commercial capacity.

PIPA protects the privacy of clients, customers, employees and volunteers by establishing the rules for the collection, use and disclosure of personal information by organizations.

The Act seeks to balance the right of the individual to have his or her personal information protected with the need of organizations to collect, use or disclose personal information for reasonable purposes. PIPA also gives individuals the right to access their own personal information held by organizations and to request corrections.

The Commissioner oversees and enforces the administration of these Acts to ensure their purposes are achieved.

The Commissioner's powers, duties and functions include:

- providing independent review and resolution on requests for review of responses to access to information requests and complaints related to the collection, use and disclosure of personal and health information;
- investigating any matters relating to the application of the Acts, whether or not a review is requested;
- conducting inquiries to decide questions of fact and law and issuing binding orders;
- educating the public about the Acts, their rights under the Acts and access and privacy issues in general;
- receiving comments from the public concerning the administration of the Acts;
- giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts;
- engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts;
- commenting on the implications for access to information or for protection of personal privacy of proposed legislative schemes and existing or proposed programs;
- commenting on the access and privacy implications of privacy impact assessments submitted to the Commissioner; and
- commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching.

Vision

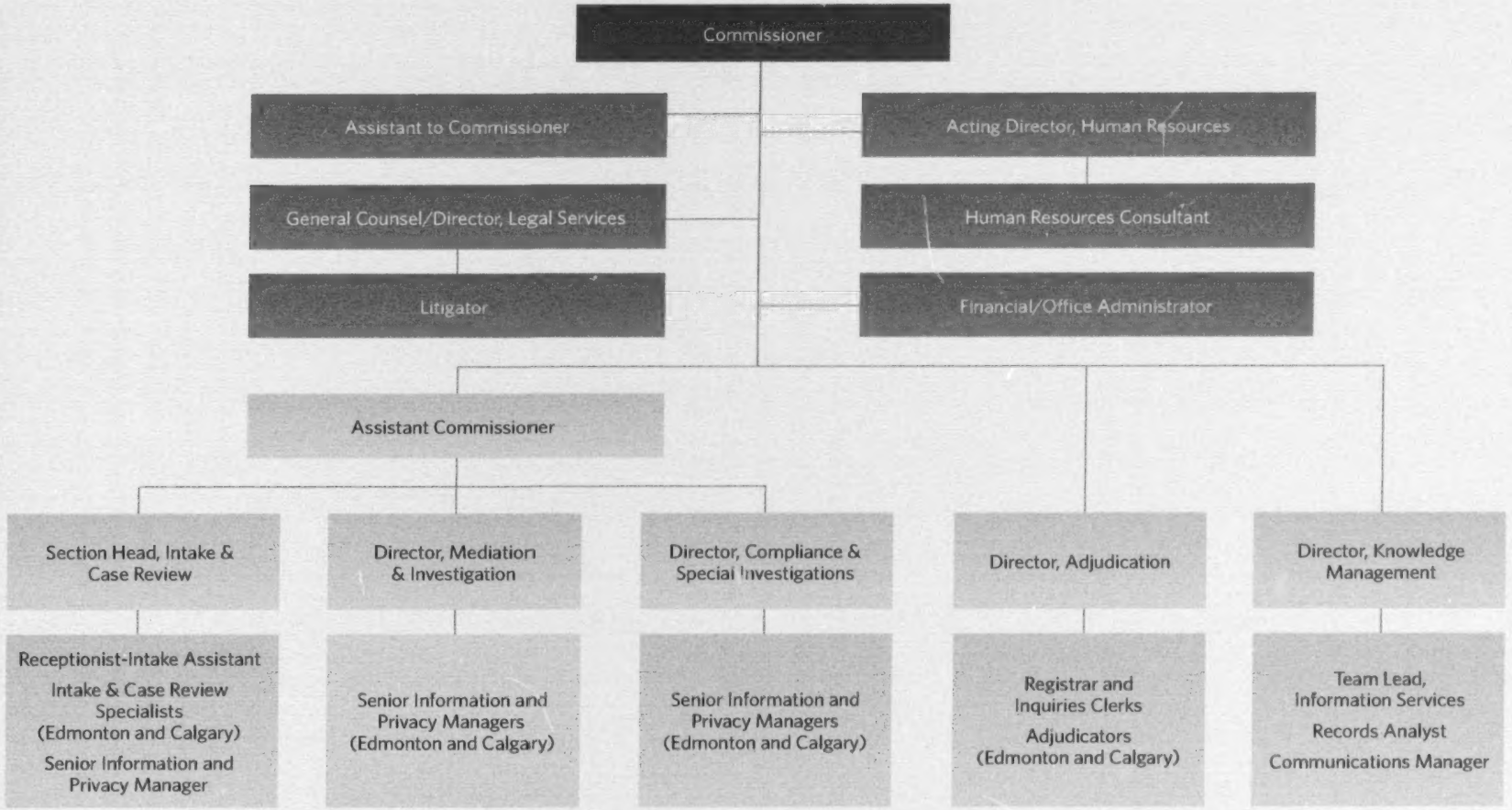
A society that values and respects access to information and personal privacy.

Mission

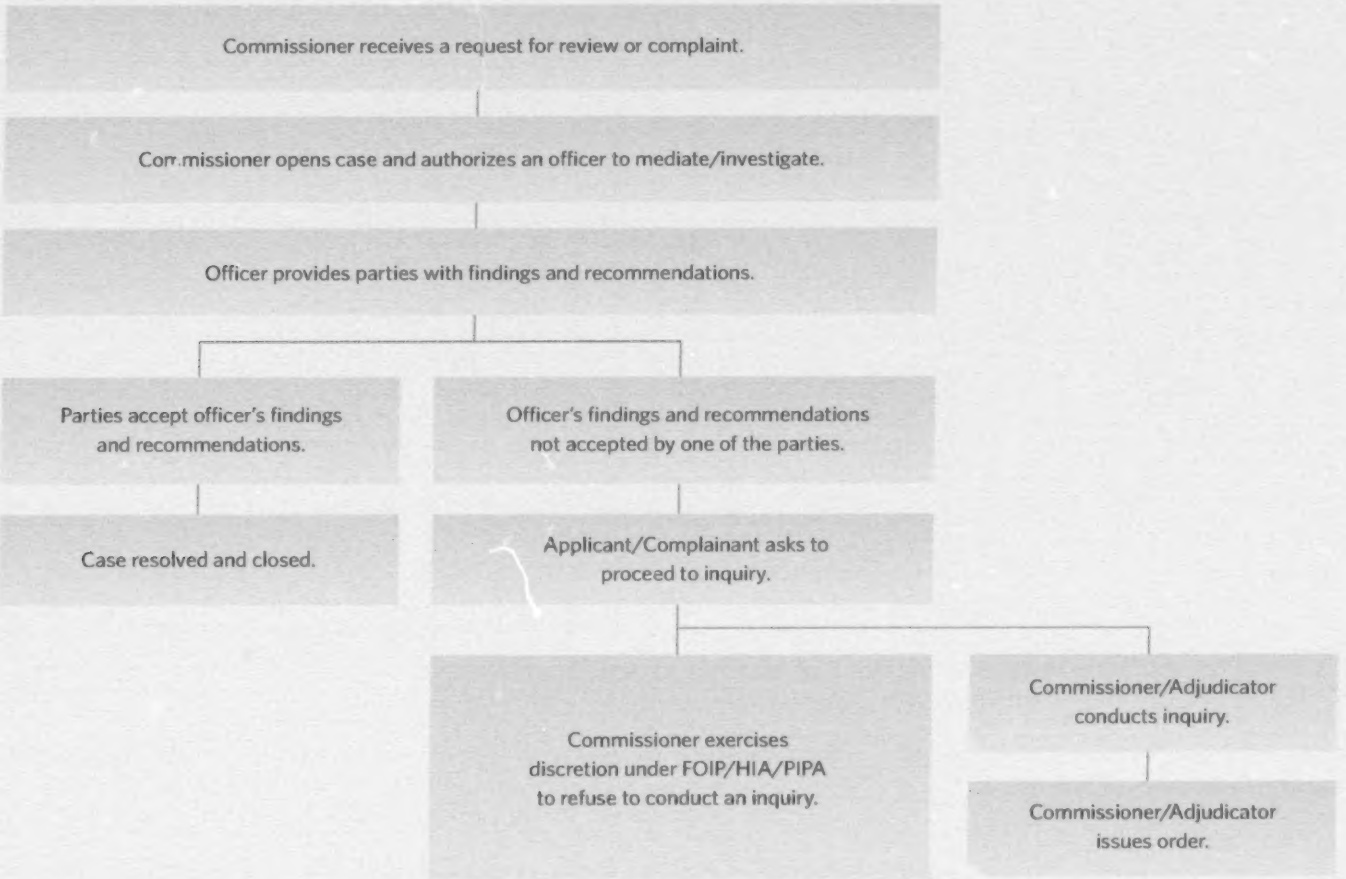
Our work toward supporting our vision includes:

- advocating for the privacy and access rights of Albertans;
- ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta; and
- providing fair, independent and impartial reviews in a timely and efficient manner.

OIPC Organizational Structure 2013-14



The Process: Request for Review/Complaint


Commissioner receives a request for review or complaint.
Commissioner opens case and authorizes an officer to mediate/investigate.
Officer provides parties with findings and recommendations.
Parties accept officer's findings and recommendations.
Officer's findings and recommendations not accepted by one of the parties.
Case resolved and closed.
Applicant/Complainant asks to proceed to inquiry.
Commissioner exercises discretion under FOIP/HIA/PIPA to refuse to conduct an inquiry.
Commissioner/Adjudicator conducts inquiry.
Commissioner/Adjudicator issues order.

OIPC as a Public Body

FOIP Requests to OIPC

Section 4(1)(d) of the FOIP Act states that records created by or for or in the custody or under the control of the Commissioner in the exercise of her legislative functions are excluded from the application of the FOIP Act.

In 2013-14, the OIPC received six requests for access to information pursuant to the FOIP Act: two general information requests and four personal information requests.

With respect to the two general information requests, the applicants were informed that the records requested were excluded from the FOIP Act under section 4(1)(d). On the four personal information requests:

- Two applicants were informed that the records responsive to their requests were excluded under section 4(1)(d) of the FOIP Act; and
- Two applicants were informed that our search failed to retrieve any responsive records.

All requests were responded to within the 30-day time limit set out in the FOIP Act.

Requests for Review

Under section 77(2) of the FOIP Act, a person who makes a request to the Commissioner for access to a record may ask an adjudicator to review any decision, act or failure to act of the Commissioner that relates to the request. To ask for a review, a written request must be delivered within 60 days of receiving notification of the Commissioner's decision on the access request (section 79(1) and section 79(2)(a)(i) of the FOIP Act) to the Minister of Service Alberta.

Upon receipt of a request for review, the Minister must as soon as practicable give the request to an adjudicator (section 80). Section 75(1) states that the Lieutenant Governor in Council may designate a judge of the Court of Queen's Bench of Alberta to act as an adjudicator.

On April 15, 2013, OIPC received written notification from the Minister of Service Alberta that an applicant had requested a review of the OIPC's response to an access request that was received in the previous fiscal year. An adjudicator was designated. This matter is still outstanding at the end of the 2013/14 fiscal year.

OIPC Privacy Breaches

In 2013-14, the OIPC conducted five internal investigations into potential privacy breaches:

- Two incidents involved documents attached in error to correspondence sent by the OIPC. The documents were retrieved by the OIPC or the recipient confirmed the documents were shredded. The personal information involved was limited to the names of individuals representing organizations in their official capacity. The disclosures presented no real risk of significant harm to the individuals affected. To prevent a recurrence of this nature, OIPC staff conducts a second check to ensure correct documents are attached before correspondence is sent;
- OIPC Human Resources could not locate a completed employee performance appraisal. A thorough search of all human resources files failed to find the missing document. The investigation found no evidence that any other individual accessed the completed performance appraisal form. As a result of the incident, OIPC Human Resources established a system to document when performance reviews are due and received;
- An internal staff email was inadvertently sent to an employee with a Commissioner's office in another jurisdiction. The other employee's first name is the same as an OIPC employee. The other employee notified OIPC immediately and confirmed that the email had been deleted. Disclosure was limited to the names and work email addresses of OIPC staff; and
- An envelope containing a signed contract was inadvertently left at Government House. The contract contained the name and address of the contractor and the financial amount of the contract. The envelope was subsequently retrieved by the OIPC, with no evidence of unauthorized access. The contractor was notified about the incident.

Proactive Travel and Expenses Disclosure

The OIPC continues to publicly disclose the vehicle, travel and hosting expenses of the Commissioner and the travel and hosting expenses of the Assistant Commissioner and OIPC Directors on a bi-monthly basis. The information is available on the OIPC's website: www.oipc.ab.ca

Financial Overview

For the 2013-14 fiscal year, the total approved budget for the OIPC was $6,867,000. The total cost of operating expenses and capital purchases was $6.2 million. The OIPC returned $643,369 (9.4% of the total approved budget) to the Legislative Assembly.

Total Actual Costs Compared to Budget

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 6,757,000	$ 6,075,438	$ 681,562
Capital Purchases	110,000	148,193	(38,193)
Total	**$ 6,867,000**	**$ 6,223,631**	**$ 643,369**

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 81% of the operating expenses budget. Due to vacant positions and staff taking fewer courses, payroll related costs were $753,195 below budget. There was a hiring freeze during a 6 month period to enable all OIPC employment positions to be reviewed for appropriate classification in accordance with the *Public Service Act*. Most of the 10 vacant positions were filled by year end or shortly thereafter.

Supplies and services were $71,633 over budget comprised of approximately $52,000 for contracted services performed by nine contractors during the hiring freeze and $26,500 over budget for special projects completed during the year, including artwork and design related to the new OIPC logo, Phase II of an OIPC stakeholder survey, enhancement of the OIPC public website, two research projects, and a Privacy Impact Assessment for the new OIPC Case Management software. Various other supplies and services were under budget a net of approximately $7,000.

Total Actual Costs Compared to Prior Year

	2013-14	2012-13	DIFFERENCE
Operating Expenses	$ 6,075,438	$ 6,166,963	$ (91,525)
Capital Purchases	148,193	15,864	132,329
Total	**$ 6,223,631**	**$ 6,182,827**	**$ 40,804**

Total costs for operating expenses and capital purchases increased by $40,804 from the prior year. This is due primarily to development and implementation of new Case Management software. There were also increased supplies and services offset by substantial payroll related savings as a result of the hiring freeze.

Trends & Issues

This section of the Annual Report, first introduced in 2012-13, is intended to provide some context for the work of the OIPC by highlighting some of the provincial, national and international issues and trends that shape and influence the access and privacy landscape, and characterize the fiscal year.

Emergencies and Disasters

Privacy breaches, complaints and delays in accessing information can result when an organization, public body or custodian switches or deviates from its normal practices—such as the result of a planned event (e.g. a move to new premises) or something that can't be controlled (e.g. an emergency or natural disaster). Whether planned or unplanned, these events can cause confusion: what action should be taken? How quickly? Who is responsible?

When processes aren't followed, or are not in place to begin with, unintended consequences can result, sometimes with significant effects on access and privacy. Many custodians, public bodies and organizations found themselves in this situation as a result of the 2013 Alberta floods—scrambling to protect and recover records and personal information.

During and after the floods, the OIPC responded to a number of calls about how to handle records and information at risk, providing advice and recommendations related to first steps (move the records to a safe and dry location, assess the extent of damage), through to ensuring the security of information when contracting with companies (such as those with expertise in recovering water-damaged records) or engaging volunteers to assist with clean-up.

Although many custodians, public bodies and organizations were caught off-guard by the floods, the risks associated with unplanned events such as emergencies and natural disasters are not unforeseeable. The best strategy for public bodies, custodians and organizations is to be prepared.

The OIPC's investigation in the wake of a fire and explosion at the Shaw Court Building in Calgary took a close look at the importance of planning for disasters. The incident affected a number of computer systems holding personal, health and financial information of Albertans. The investigation examined the safeguards that public bodies, health custodians and businesses had in place to protect personal and health information affected by the incident at Shaw Court, and the measures taken to protect information while restoring access to services. The report, released in October 2013, made a number of recommendations, emphasizing the need to:

- establish a planning process;
- perform a business impact analysis and review it regularly;
- prepare plans to continue operations and recover from a disaster, based on criticality of systems;
- approve and distribute plans;
- train those directly involved in the plan and test plans regularly; and
- revise and refine plans, based on test results and changing business requirements.

Another key component of a disaster response or business continuity plan is to consider how information can and should be shared in the event of an emergency or disaster. Uncertainty around the sharing of personal information in an emergency situation can result in unnecessary confusion and delays. The consequences of failing to share information can be significant, as documented in reviews of certain high-profile situations such as the Asian Tsunami in 2004 and Hurricane Katrina in 2005.

Privacy laws should not be considered a barrier to appropriate information sharing, nor should they be used as an excuse for inaction. In fact, each of Alberta's privacy laws contains provisions to allow for the sharing of personal or health information in the event of an emergency or disaster.

In May 2013, the Alberta OIPC collaborated with the Federal Privacy Commissioner and Provincial and Territorial Commissioners on a "Privacy Emergency Kit". The "Kit" is intended to help organizations, public bodies and custodians enhance the timeliness and content of communications during an emergency while giving people confidence that their personal information will be handled appropriately. It contains materials that were developed to address the sharing of personal information in emergency situations such as hurricanes and other natural disasters, pandemics or other health related crises and situations such as terrorist attacks and explosions. The "Kit" is based on a resolution adopted by the International Conference of Data Protection and Privacy Commissioners in 2011.

Information Sharing

We increasingly see public bodies, private sector and not-for-profit organizations, and health care custodians working together to provide programs and services to Albertans. Information sharing plays a vital role in effectively and efficiently delivering these programs and services.

Access and privacy laws allow for information sharing in almost every circumstance where you might think it is required. The FOIP Act, HIA, and PIPA all recognize that information can and should be shared in some circumstances. Each law sets out the circumstances in which personal and health information may be disclosed, either with or without consent. Section 40(1) of the FOIP Act, for example, lists 38 circumstances in which personal information may be disclosed. In addition, other laws occasionally override the FOIP Act or otherwise authorize information sharing.

Despite these provisions, the OIPC frequently hears that information is not shared because employees do not understand their legislative authority or are fearful of contravening privacy laws. To address this, proposals and initiatives seeking to address information sharing needs sometimes suggest removing discretionary information-sharing provisions in favor of mandatory disclosure requirements, reducing consent requirements, and expanding authorities for indirect collection. Solutions of this kind have the potential to seriously undermine individual access and privacy rights if they are implemented in a piecemeal fashion, without regard to the legislative framework as a whole and without due consideration of appropriate controls.

At their very core, access and privacy laws are about providing individuals with control over how their personal information is collected, used, and disclosed. The exercise of access and privacy rights fundamentally depends on transparency – it is impossible to complain about the collection of your personal information if you don't know it has been collected; similarly, it is impossible to access your personal information if you don't know which entities hold it.

Authorizing information sharing for broad purposes that are open to interpretation, and difficult to anticipate secondary uses, leads to confusion and complaints. Sharing more information than is necessary increases the potential risk of harm in the event of a privacy breach. Even more significantly harmful is sharing information with other entities—such as some non-profit service providers in Alberta—that are not subject to any access and privacy legislation.

Amending established access and privacy laws, introducing paramountcy provisions, or enacting stand-alone legislation to work around perceived legislative obstacles have the potential to introduce new tests, inconsistencies and confusion, ultimately undermining existing access and privacy laws and increasing reluctance to share information.

The Information and Privacy Commissioner raised concerns about information sharing initiatives in a number of forums in 2013, including: public comments on Bill 25, the *Children First Act*, introduced in the Legislative Assembly in May 2013; presentations delivered during Right to Know Week; and, the Commissioner's submission to the government review of the FOIP Act.

In all cases, the message has been consistent: information sharing is vital to providing programs and services that will benefit all Albertans, but this does not have to come at the expense of access and privacy rights.

Among other things, the Commissioner has recommended:

- Ensure that all participants in cross-sectoral information sharing initiatives are subject to Alberta's access and privacy laws.
- Require mandatory privacy impact assessments for certain information sharing activities (e.g. data matching, cross-sectoral initiatives) to ensure they are thoroughly reviewed and assessed for access and privacy implications.
- Ensure that legislative amendments to facilitate information sharing are harmonized among the FOIP Act, HIA, and PIPA to avoid introducing inconsistencies.
- Establish a registry of information sharing initiatives with the OIPC or a designated government ministry to document:
  - the nature of the information sharing initiative;

- names of participating stakeholders; and
- contact information of an officer/employee who can answer questions about the collection, use, disclosure, retention, security, or destruction of personal/health information.

Regularly update the registry and make it easily accessible to the public.

- Require participants in information sharing initiatives to record disclosures, and maintain records documenting:
  - the name of the person/service provider to whom the information was disclosed;
  - the date and purpose of the disclosure; and
  - a description of the information disclosed.
- Ensure that individuals who are the subject of the information sharing have an express, legislated right to ask for access to and a copy of the disclosure notes. Individuals should also have a right to ask the Commissioner for a review in relation to their requests.

To facilitate a greater awareness of both the benefits and potential risks of information sharing initiatives, in 2013 the OIPC commissioned research into the subject. The results of this research are expected to be made publicly available in 2014.

Requests to excuse fees

33 requests received; **27** closed; **6** still open

Requestor type: 15 opposition/political (45%); 6 individuals (18%); 9 interest groups (27%); 3 media (9%)

Disposition:

- Confirmed public body decision to deny fee waiver: 5 (19%)
- Request abandoned/withdrawn: 7 (26%)
- Fees waived in full/part: 13 (48%)
- No jurisdiction/other: 2 (7%)

Thirty-three cases were received in 2013-14. To date, 27 have been closed (over 2013-14 and 2014-15).

Focus on Access

The OIPC's 2012-13 Annual Report identified a renewed focus on access to information issues, particularly with regard to the expense claims of senior health officials; the proactive disclosure of travel and hospitality expenses of cabinet ministers, senior officials and others; and the Government of Alberta's launch of its review of the FOIP Act.

The trend continued in 2013-14. Some key events in Alberta:

- May 2013: the Alberta Government launched its Open Data Portal;
- October 2013: following an access to information request and review by the OIPC, information about severance provided to the former Premier's Chief of Staff was made public. This was followed by an announcement that the government would be implementing a policy to expand the proactive disclosure of salary and severance information for senior government employees. The first disclosures were made in January 2014;
- November 2013: based on information released following an order issued by the OIPC in June 2013, the *Edmonton Journal* and *Calgary Herald* published a series of articles related to the deaths of children in care, revealing that the government had previously under-reported the number of deaths. Additional information was released in January 2014. At the same time, the government hosted a roundtable discussion to look at issues associated with the child welfare system in Alberta, including the publication ban provisions in the *Children, Youth and Family Enhancement Act*.

The number and type of cases opened by the OIPC also demonstrated a focus on access-related matters. Although the total number of FOIP cases opened in 2013-14 was on par with 2012-13 (a 2% increase), the OIPC saw:

- a 27% increase in the number of requests for review (17% the previous year);

- a 19% increase in the number of requests to the Commissioner for time extensions (time extension requests have increased 125% over the last three years, with 2012-13 seeing an 89% increase in one year);
- the number of requests to excuse fees increased from 3 in 2012-13 to 33 in 2013-14 (a 1,000% increase).

At the same time, privacy-related complaints and self-reported breaches under the FOIP Act decreased by 27% and 46% respectively.

After an increase of 115% last year, the number of third party requests for review decreased in 2013-14 by almost 40%, possibly due to a shift from access requests that focus on expense information of third parties, to more general requests for government records.

Legislative Reform

Fiscal year 2013-2014 saw significant attention to legislative reform of all three of Alberta's access and privacy laws.

The GoA review of the FOIP Act

In 2013, the GoA initiated a consultation and review of Alberta's FOIP Act. The Information and Privacy Commissioner made two submissions to this process. The first submission, *Becoming a Leader in Access and Privacy*, sets out ideas, suggestions and recommendations to help Alberta become a leading example to other jurisdictions in access and privacy legislation. Some of the key recommendations include:

- Review the **scope** of the FOIP Act to ensure that publicly-funded entities that should be captured are, and confirm the ongoing need for exclusions;
- Review the **exceptions to access** set out in the FOIP Act to ensure they are as narrow and limited as possible;
- Ensure adequate resources are allocated to educating the public and stakeholders about the FOIP Act;
- Ensure that fees are appropriate and not a barrier to access;
- Require public bodies to identify categories of records that will be made publicly available without requiring formal access requests (**proactive disclosure**). Require public bodies to make these records available;
- Require that **cross-sectoral information sharing initiatives be registered** with the OIPC or a designated government ministry and ensure that all participants are subject to Alberta's information and privacy laws;
- Require participants in information sharing initiatives to **document personal information disclosures**. Ensure individuals have a legislated right to access the disclosure notes, and request a review by the Commissioner;
- Ensure an appropriate statutory and policy framework for records and information management is in place to support transparency, accountability and compliance with the FOIP Act. This could include amending the FOIP Act to require that public bodies:
  - create such records as are reasonably necessary to **document their decisions, actions, advice, recommendations and deliberations**
  - ensure that all records are covered in **records retention and disposition schedules**
- Require public bodies to complete and submit **privacy and access impact assessments** to the OIPC on proposed initiatives, schemes or programs that meet certain criteria (e.g. information sharing initiatives, data matching initiatives); and
- Require public bodies to **report privacy incidents** meeting certain criteria to the OIPC and give the Commissioner the power to require public bodies to **notify affected individuals.**

The Commissioner's second submission, *Making the FOIP Act Clear, User-Friendly and Practical*, provided comments and recommendations relating to technical aspects of the FOIP Act.

At the time of writing, the Government of Alberta has not announced how it will move forward with amendments to the legislation.

PIPA Constitutional Amendment

In November 2013, the Supreme Court of Canada released its decision in *Alberta (Information and Privacy Commissioner) v. the United Food and Commercial Workers (UFCW), Local 401* (2013 SCC 62), ruling that Alberta's PIPA is unconstitutional and declaring it invalid. The Court gave the Alberta Legislature 12 months to bring the Act in line with the *Canadian Charter of Rights and Freedoms*.

Despite striking down PIPA, the Supreme Court decision provides some clarification as to the balancing of two important rights: a union's freedom of expression as against personal privacy rights. In so doing, the Court also:

- acknowledged privacy as an evolving "quasi-constitutional" right worthy of protection;
- pointed out that the ability of individuals to control their personal information is "intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy";
- recognized that this objective is increasingly significant today, where new technologies give organizations an almost unlimited capacity to collect, use and disclose personal information; and
- recognized that by merely appearing in public, an individual does not automatically forfeit his or her interest in retaining control over personal information.

In January 2014, the Information and Privacy Commissioner wrote to the Government of Alberta proposing a solution that would address the constitutional problems with PIPA while also preserving an appropriate degree of protection for the personal information of Albertans.

The Commissioner recommended an exception to consent for the collection, use and disclosure of personal information by unions for expressive purposes in the context of picketing during a lawful strike. Instead of completely excluding these activities from the Act, an exception to consent ensures that personal information is still subject to other provisions of the Act—including the duty to safeguard, individual rights of access and correction, and independent review by the Commissioner.

The Commissioner urged the government to move quickly on this matter so as to meet the Supreme Court's timeline and to maintain the personal privacy protections Albertans have come to expect.

Breach reporting and notification in the health sector

In January 2014, Medicentres Canada Inc. notified the media and the public of an incident involving the theft of an unencrypted laptop containing billing information for 631,000 Albertans. The Information and Privacy Commissioner subsequently announced an investigation of the incident, as well as a broader review of the way privacy breaches are reported in the health sector in Alberta.

The incident served to draw attention to the importance of including privacy breach reporting and notification requirements in access and privacy legislation.

In February 2014, the Commissioner wrote to the Minister of Health to formally request the Government of Alberta consider amending HIA to include mandatory breach reporting and notification provisions.

The Commissioner's letter noted that, in Canada, nine jurisdictions have passed or introduced broadly focused health privacy legislation and of those, six include mandatory breach reporting or notification provisions.

The letter also identified issues that should be considered when designing an appropriate breach reporting and notification legislative scheme, including: who should be notified about a breach, what the triggers are for notification, what should be reported and in what time frame, and whether there should be penalties, sanctions or other consequences for failing to notify.

It was also noted that, of the province's three access and privacy laws, only Alberta's private sector law, PIPA, requires an organization to report a privacy breach and gives the Commissioner the power to require the organization to notify affected individuals.

The Commissioner recommended similar amendments be considered for health custodians under the HIA. Including privacy breach notification and reporting requirements in all three of Alberta's access and privacy laws is an important component of protecting Albertan's privacy rights and will help to put Alberta at the forefront of privacy protection.

By the Numbers

74
orders issued
(68% increase from 2012-13)

117
media enquiries
(46% increase from 2012-13)

73
speeches and
presentations delivered
(16% decrease from 2012-13)

369
Privacy Impact Assessments
submitted by HIA custodians
(8% decrease from 2012-13)

303
requests for review opened under FOIP

27%
increase from 2012-13

46
requests for review opened under HIA

229%
increase from 2012-13

75
complaints opened under PIPA

44%
increase from 2012-13

Number of self-reported breach cases opened:

FOIP **22**
(46% decrease
from 2012-13)

HIA **68**
(19% increase
from 2012-13)

PIPA **96**
(14% increase
from 2012-13)

2042
total number
of cases opened
(606 intake cases)

1706
total number
of cases closed
(547 intake cases)

Statistics Reported by OIPC

A new organization structure for the OIPC was implemented in 2013-2014. As a result of the restructuring, the legislation-based teams (FOIP, HIA and PIPA) were consolidated into functional teams that encompassed all three Acts: the Mediation and Investigation (MI) team, the Compliance and Special Investigations (CSI) team and the Intake and Case Review (ICR) unit.

The MI team is authorized to investigate and try to resolve matters that come to the OIPC. MI is an integral component to the Commissioner's legislative mandate to provide independent review of decisions made by public bodies, custodians and private sector organizations.

The CSI team expands on work related to privacy impact assessments, self-reported breaches, investigations generated by the Commissioner and offence investigations. CSI reviews and investigates public bodies, custodians and private sector organizations for compliance with the three Acts by conducting compliance investigations and auditing systems, practices and operations for access and privacy implications.

The establishment of the ICR unit recognizes and formalizes casework performed by our intake staff. The cases include determining whether parties coming to the OIPC are properly exercising the rights set out in Alberta's three access and privacy laws; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints. The work performed by the ICR unit is essential in establishing the jurisdiction and the authority for matters to proceed to mediation, investigation and adjudication.

Intake cases have not been included in statistics reported in OIPC's previous annual reports. However, to provide a more comprehensive picture of the work that is performed by the OIPC, we have included intake case statistics in the 2013-2014 Annual Report:

- The "Sub-Totals" reported in Table 1 (Cases Opened by Case Type) and Table 2 (Cases Closed by Case Type) are comparable with statistics reported in previous annual reports. The new "Overall Totals" incorporate the intake case statistics.
- Graph A (Total Cases Opened - Three Year Comparison) and Graph B (Total Cases Closed - Three Year Comparison) provide a comparative analysis with statistics reported in previous annual reports but the totals for 2013-14 include the intake case statistics.

Of the 606 intake cases opened:

416 (or 69%) were under FOIP
80 (or 13%) were under HIA
110 (or 18%) were under PIPA

547 intake cases were closed:

392 (or 72%) under FOIP
71 (or 13%) under HIA
84 (or 15%) under PIPA

Table 1: Cases Opened by Case Type

FOIP	2013-14	2012-13	2011-12
Advice and Direction	1	4	0
Authorization to Disregard a Request	0	3	4
Complaint	91	125	65
Disclosure to Commissioner (Whistleblower)	1	-	-
Notification to OIPC	4	6	1
Engage in or Commission a Study	2	0	0
Excuse Fees	33	3	6
Investigation Generated by Commissioner	5	11	7
Offence Investigation	0	1	1
Privacy Impact Assessments	14	21	22
Request Authorization to Indirectly Collect	1	-	-
Request for Information	26	32	34
Request for Review	303	239	205
Request for Review 3rd Party	26	43	20
Request Time Extension	81	68	36
Self-reported Breach	22	41	24
Sub-Total	**610**	**597**	**425**
Intake Cases	**416**	**N/R**	**N/R**
Overall Total	**1026**	**597**	**425**

HIA	2013-14	2012-13	2011-12
Advice and Direction	0	0	1
Authorization to Disregard a Request	0	0	1
Complaint	50	27	17
Notification to OIPC	0	1	0
Engage in or Commission a Study	0	0	1
Excuse Fees	0	0	0
Investigation Generated by Commissioner	15	48	15
Offence Investigation	4	0	2
Privacy Impact Assessments	369	399	434
Request for Information	33	48	52
Request for Review	46	14	28
Request Time Extension	0	0	0
Self-reported Breach	68	57	59
Sub-Total	**585**	**594**	**610**
Intake Cases	**80**	**N/R**	**N/R**
Overall Total	**665**	**594**	**610**

PIPA	2013-14	2012-13	2011-12
Advice and Direction	0	1	0
Authorization to Disregard a Request	0	1	0
Complaint	75	52	82
Notification to OIPC	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	2
Investigation Generated by Commissioner	14	6	2
Offence Investigation	0	0	0
Privacy Impact Assessments	1	0	1
Request for Information	3	10	10
Request for Review	52	56	61
Request Time Extension	0	0	0
Request for Advance Ruling	0	0	1
Self-reported Breach	96	84	94
Sub-Total	**241**	**210**	**253**
Intake Cases	**110**	**N/R**	**N/R**
Overall Total	**351**	**210**	**253**

N/R - not reported

Note: see Appendix A for a listing of cases opened in the 2013-14 fiscal year

Note: only FOIP allows a 3rd party to request a review of a decision to release 3rd party information to an applicant

Table 2: Cases Closed by Case Type

FOIP	2013-14	2012-13	2011-12
Advice and Direction	1	3	0
Authorization to Disregard a Request	1	3	4
Complaint	77	66	68
Disclosure to Commissioner (Whistleblower)	1	-	-
Notification to OIPC	4	6	1
Engage in or Commission a Study	0	0	0
Excuse Fees	12	3	6
Investigation Generated by Commissioner	6	2	11
Offence Investigation	0	1	1
Privacy Impact Assessment	13	15	24
Request Authorization to Indirectly Collect	1	-	-
Request for Information	22	33	41
Request for Review	258	163	159
Request for Review 3rd Party	26	21	18
Request Time Extension	90	58	41
Self-reported Breach	21	37	20
Sub-Total	**533**	**411**	**394**
Intake Cases	**392**	**N/R**	**N/R**
Overall Total	**925**	**411**	**394**

HIA	2013-14	2012-13	2011-12
Advice and Direction	0	0	1
Authorization to Disregard a Request	0	1	0
Complaint	15	23	26
Notification to OIPC	0	1	0
Engage in or Commission a Study	0	1	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	13	42	14
Offence Investigation	0	1	16
Privacy Impact Assessment	344	410	419
Request for Information	29	49	54
Request for Review	17	17	33
Request Time Extension	0	0	0
Self-reported Breach	40	59	51
Sub-Total	**458**	**604**	**614**
Intake Cases	**71**	**N/R**	**N/R**
Overall Total	**529**	**604**	**614**

PIPA	2013-14	2012-13	2011-12
Advice and Direction	0	1	0
Authorization to Disregard a Request	0	0	1
Complaint	50	113	135
Notification to OIPC	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fees	0	1	2
Investigation Generated by Commissioner	4	2	1
Offence Investigation	0	0	0
Privacy Impact Assessment	0	0	1
Request for Information	7	7	8
Request for Review	41	56	72
Request Time Extension	0	0	0
Request for Advance Ruling	0	0	1
Self-reported Breach	66	75	91
Sub-Total	**168**	**255**	**312**
Intake Cases	**84**	**N/R**	**N/R**
Overall Total	**252**	**255**	**312**

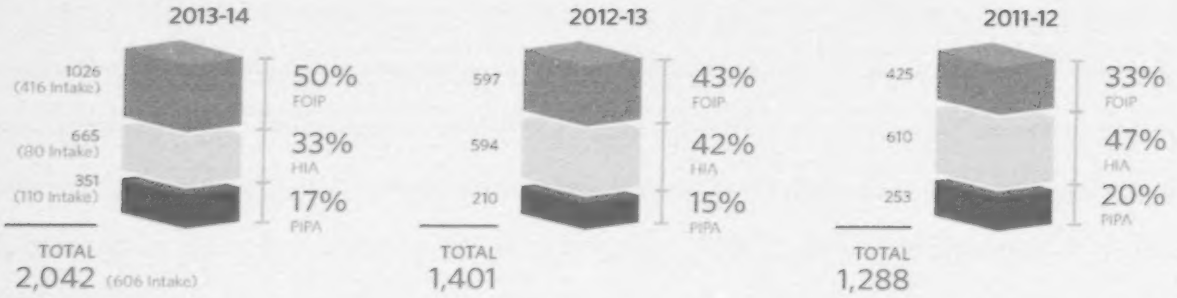
N/R - not reported

Note: see Appendix B for a listing of the cases closed in 2013-14

Note: only FOIP allows a 3rd party to request a review of a decision to release 3rd party information to an applicant

Graph A: Total Cases Opened

Three Year Comparison



Graph B: Total Cases Closed

Three Year Comparison

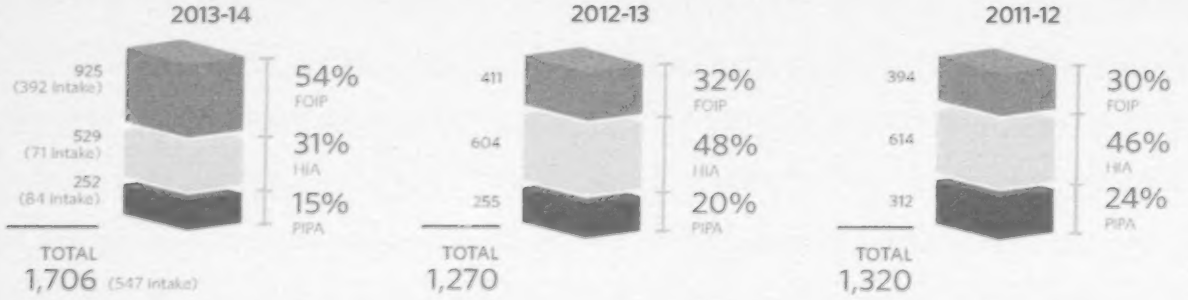


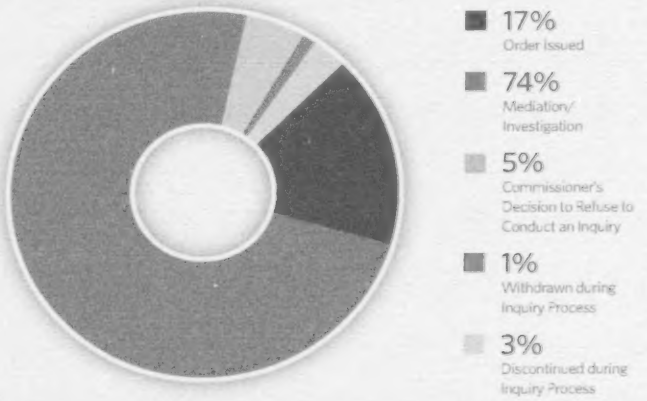
Table 3:
Percentage of Cases Closed by Resolution Method

Under the Acts, only certain case types can proceed to inquiry if the matters are not resolved at mediation/investigation. The statistics below are those case types that can proceed to inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Resolved by Mediation/Investigation	261	27	79	367	74%
Resolved by Order	70	3	10	83	17%
Resolved by Commissioner's Decision to Refuse to Conduct an Inquiry	22	1	1	24	5%
Withdrawn during inquiry process	7	0	0	7	1%
Discontinued during inquiry process	13	1	1	15	3%
Total	**373**	**32**	**91**	**496**	**100%**

FOIP Orders: 61 (70 cases); HIA Orders: 3 (3 cases); PIPA Orders: 10 (10 cases)

Graph C: Percentage of Cases Closed by Resolution Method



Of the 496 cases that could proceed to inquiry:

26% were resolved within 90 days

21% were resolved within 91 to 180 days

53% took more than 180 days to resolve.

Notes: (1) Three (3) discontinued FOIP files were re-opened. (2) Commissioner refused to hear an inquiry for 18 connected files after conducting an inquiry on the file that included everything in the other 18 files. (3) An inquiry combining an HIA file and a PIPA file was discontinued. (4) Some Orders and/or Report Numbers were assigned to more than one case. Some cases had more than one Order. (5) Orders are recorded by the date the Order was signed, rather than the date the Order was publicly released. (6) This table only includes Orders issued that concluded/closed the file. (7) An inquiry can be discontinued due to a lack of contact with or participation of the applicant or complainant or the issues have become moot.

See Appendix C for a list of Orders, Decisions and Public Investigation Reports issued in 2013-14
A copy of all Orders, Decisions and Public Investigation Reports are available on the OIPC website: www.oipc.ab.ca

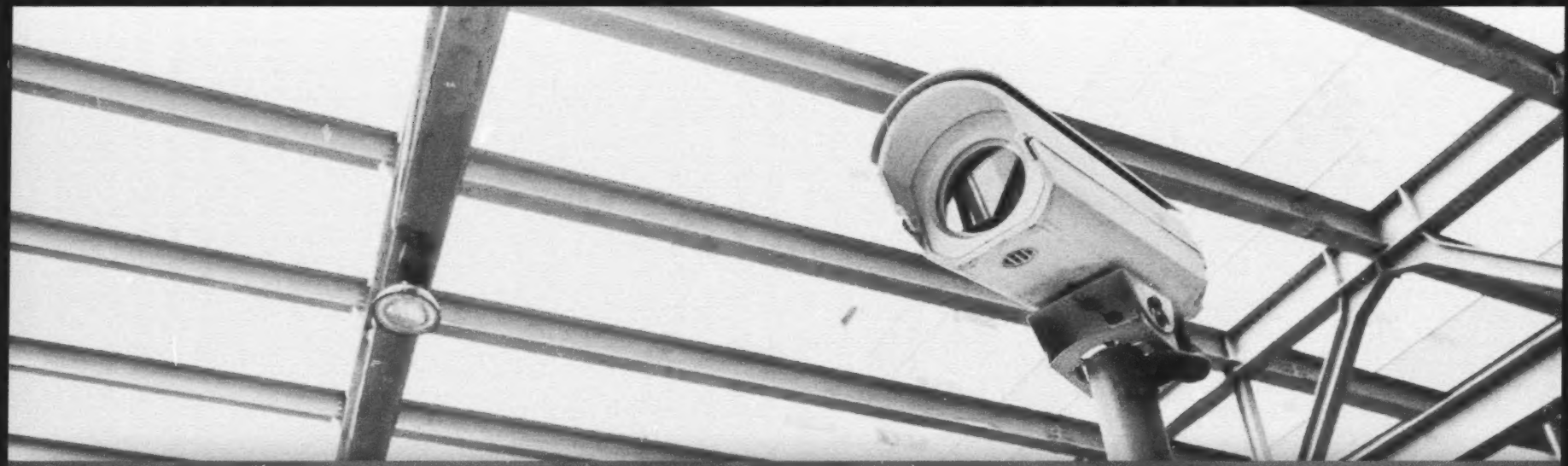
Table 4: Telephone Calls, Emails and Written Enquiries 2013-14

FOIP	Number	Percentage
Public Bodies	197	23%
Individuals	651	77%
Total	**848**	

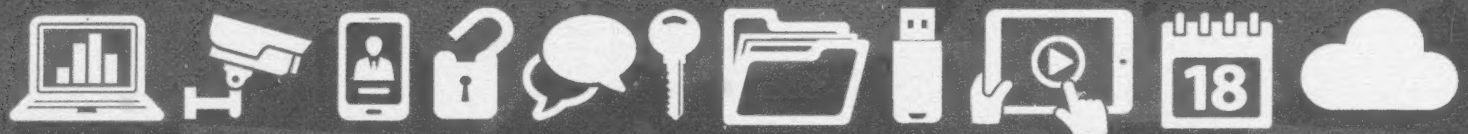
HIA	Number	Percentage
Custodians	322	39%
Individuals	514	61%
Total	**836**	

PIPA	Number	Percentage
Organizations	517	30%
Individuals	1,216	70%
Total	**1,733**	

Emails	**450**
Non-jurisdictional	**155**
Total	**4,022**



Regulation & Enforcement



Requests for Time Extensions under FOIP

The OIPC has seen a **125**% increase in time extension requests since 2011-12.

Under section 11(1)(a) of the FOIP Act, a public body must make every reasonable effort to respond to a request no later than 30 calendar days after receiving the request, unless the time limit for response is extended under section 14.

Section 14(1) allows a public body to extend the time limit for responding by up to 30 days on its own authority in certain circumstances. An extension period longer than an additional 30 days requires the Commissioner's permission.

Section 11(2) states a failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under section 14, is to be treated as a decision to refuse to access.

In seeking permission from the Commissioner to extend the response due date, a public body must establish that one of the conditions set out in section 14 has been met. Furthermore, since the FOIP Act is premised on timely processing of requests, an extension must be reasonable given the relevant circumstances.

In 2013-2014, the OIPC received a total of 81 requests for permission to extend the response due date:

- 35 requests (or 43%) were granted as requested;
- 20 requests (or 25%) were partially granted (extension period permitted less than the period requested by the public body);
- 21 requests (or 26%) were refused; and
- 5 requests (or 6%) were withdrawn by the public bodies.

Of the 81 time extension requests received by the OIPC:

77% were made by provincial government ministries

11% were made by municipalities

5% were made by Child and Family Service Authorities

Post-secondary institutions, Boards and Commissions each made 2%

Mandatory Breach Reporting under PIPA

Under PIPA, organizations must report to the Commissioner any unauthorized loss, access or disclosure of personal information, where the organization determines a real risk of significant harm may result to the individuals concerned. Further, the Commissioner has the power to require organizations to notify affected individuals when a privacy breach presents a real risk of significant harm.

The following highlights significant privacy breaches and trends reported under PIPA in 2013-14 and the Commissioner's decisions regarding notification.

Hacking

The Commissioner received several reports of privacy breaches resulting from hacking. In one notable case, the Commissioner required the organization to notify individuals, despite the fact the personal information was encrypted. An online retail organization sales system was attacked by a hacker, compromising names, addresses and credit card information for 33,588 Canadians, including 4,386 Albertans. Following a forensic examination, however, the organization was informed that the hacker could have the technical ability to decrypt the information. The organization recognized the elevated risk and notified the affected individuals. In coming to her decision to require notification, the Commissioner considered the possibility that the hacker may have had the ability to decrypt the personal information as a significant factor.

Tibo Distribution Inc., P2013-ND-42

Risk of phishing

Malicious software and intrusions often expose large databases of individual information to unauthorized parties. In some cases, the personal information seems innocuous—usernames, emails or names. However, when this information falls into the wrong hands, the affected individuals are vulnerable to phishing attacks. Phishing is a term used to describe an attempt by a malicious party to masquerade as an organization an individual has previously dealt with to convince him or her to divulge personal or financial information. Phishing is normally perpetrated via email, but can also be done via other electronic messaging systems.

Three breaches affecting large numbers of individuals were reported this year where the Commissioner recognized an elevated phishing risk. As an example, the Commissioner received a privacy breach report from an organization that had experienced an intrusion that compromised individuals' names, emails, hashed and salted (i.e. scrambled with a mathematical algorithm) passwords, gender and other internal identifiers. Several million individuals were affected worldwide including 1.69 million Canadians and over 400,000 Albertans (estimated). The information involved was of low to moderate sensitivity and the organization took measures to reduce the risk of harm. However, the incident involved a deliberate attack and affected a significant number of individuals. Further, the organization recognized that, given time, the hashed passwords could be reverse-engineered. Because of the malicious intent of the attacker and the large number of individuals affected, the Commissioner concluded that the risk of phishing was elevated and required the organization to notify the affected individuals.

LivingSocial Canada Enterprises Inc., P2013-ND-31;
Blizzard Entertainment Inc., P3013-ND-11;
The Certified General Accountants' Association of Alberta, P2013-ND-41

Theft or loss of mobile devices

Mobile devices, like laptop computers and USB storage drives, are especially vulnerable to theft and loss. As such, these devices need to be properly encrypted if they contain personal information. The Commissioner continues to receive reports about unencrypted mobile devices going missing. In one incident reported to the OIPC this year, an accounting firm was required to notify 285 Albertans whose electronic tax returns were stolen from an employee's vehicle. Unfortunately, the returns were stored on an unencrypted USB backup drive. Given the sensitivity of the personal information, the malicious intent of the thief and the fact the information was not encrypted, the Commissioner determined that the

affected individuals were at real risk of significant harm and required notification.

Heyrock Chartered Accountants, P2014-ND-55

Social engineering

Social engineering refers to an attempt to gain access to secured information by deceiving someone with authorized access into providing it. The following example was experienced by an organization that offers a computer system used by auto dealers to communicate with potential lenders and insurers. A caller posing as the organization's technical support contacted two employees of an auto dealer and convinced them to provide their login credentials. As a result, the fraudulent caller was able to log in to the organization's system and obtain credit report information about eight individuals. Fortunately, the organization detected the breach and prevented the attacker from going any further or accessing any more personal information, but because of the criminal intent and the sensitivity of the information, the Commissioner required the organization to notify the 8 affected individuals. This incident is a good reminder for information brokers who provide system access to users outside their organization of the need to educate these external users about how to recognize and prevent social engineering attacks.

DealerTrack Canada Inc., P2013-ND-22

In 2013-14, the Commissioner issued 36 decisions under PIPA requiring organizations to notify affected individuals about privacy breaches.

Personal information exposed within organizations

Personal information is not always compromised as the result of malicious activity. In two cases reported this year, organizations inadvertently exposed employee information on internal systems. These incidents point to the need for strong internal controls regarding the use and sharing of personal employee information.

Mars Canada Inc., P2013-ND-48; *Dominion of Canada General Insurance Company,* P2013-ND-08

Privacy Breach Reporting under FOIP and HIA

Reporting breaches under the FOIP Act and HIA is voluntary. Each year, the OIPC receives breach reports from public bodies and custodians subject to these statutes. In most cases, the OIPC works with the reporting body to ensure the breach has been stopped, causes identified, and that reasonable steps have been taken to prevent reoccurrence. In each case, the OIPC strongly encourages public bodies and custodians to notify the affected individuals about the breach; however, notification is not mandatory. If a reporting body refuses to notify individuals or delays notification, the Commissioner may launch an investigation and publish an investigation report, which serves to inform and educate the public. In some cases, where the circumstances warrant, the Commissioner may initiate investigations into possible offences, based on information received through a voluntary breach report. The Commissioner has recommended that the government implement mandatory breach notification under the FOIP Act and HIA, similar to the notification regime under PIPA.

HIA

This year, the OIPC received 68 reports of privacy breaches from custodians under HIA. The kinds of incidents reported in the health sector include lost and stolen unencrypted mobile devices, misdirected faxes, letters and emails, paper records stolen from offices and vehicles, improper disposal of health information, and inappropriate access to electronic health records systems. Custodians in the health sector have a good record of taking privacy breaches seriously and move quickly to remediate the problem, administer discipline where appropriate and inform affected individuals.

It is unfortunate that the health sector continues to experience privacy breaches involving misdirected fax and letters when more secure electronic systems are widely available.

It is equally unfortunate that the health sector continues to lose health information stored on unencrypted mobile devices, despite repeated warnings and public

investigation reports issued from the OIPC since 2006. Notably, in October 2013, Medicentres Inc. reported the theft of an unencrypted laptop containing health information on over 600,000 individuals. Medicentres eventually notified the public about the incident in January 2014 and the Commissioner subsequently launched an investigation on her own motion and committed to releasing a public investigation report. The investigation results will be highlighted in next year's annual report.

FOIP

Public bodies subject to the FOIP Act informed the Commissioner about 22 privacy breaches in 2013-14. It was of continuing concern to see the large proportion of these breaches (7/22 or 1/3) are caused by public bodies' failure to encrypt mobile devices. A number of these public bodies had encryption policies in place but the employee concerned did not implement encryption, or the policies were not enforced. Another major cause of breaches in the public sector was misdirected emails and mishaps involving cc and bcc fields in emails, pointing to a need for more education and awareness training for employees.

Offence Investigations

In 2013-14, the Commissioner initiated four investigations into possible offences under section 107 of HIA. Section 107 makes it an offence for any person to knowingly gain or attempt to gain access to health information, or collect, use or disclose health information in contravention of HIA. In each case, the allegations involve inappropriate use of information by authorized users of electronic health records systems. On a positive note, each incident was discovered by the responsible custodian and promptly reported to the OIPC. The reporting custodians are cooperating with these ongoing investigations.

Offence investigations are resource and time intensive, typically taking two years from opening to prosecution and conviction. Not all offence investigations lead to prosecutions. In some instances, there may not be enough evidence to proceed to a conviction or it can be difficult to show beyond a reasonable doubt that the alleged perpetrator acted "knowingly." Results of successful offence prosecutions will be highlighted in next year's annual report.

Privacy Impact Assessment Reviews

A privacy impact assessment (PIA) is an exercise in critical thinking and due diligence that describes how new initiatives affect the privacy of individuals. A PIA typically includes an analysis of the legal authority to collect, use, or disclose health or personal information, an assessment of privacy risk and mitigation plans, along with supporting policies and evidence that a privacy management structure is in place.

PIA Overview

Under section 64 of HIA, custodians must submit PIAs to the Commissioner before implementing a new system or administrative practice that affects individuals' health information. Under the FOIP Act and PIPA, PIA submission is not mandatory, but encouraged.

The OIPC accepted 337 PIAs in 2013-14. As usual, the vast majority of these PIAs were submitted under the mandatory PIA provision of HIA. However, 11 of the PIAs the OIPC reviewed and accepted were submitted by public bodies under the FOIP Act.

A common theme observed this year was information sharing across jurisdictions, where health information was shared with public bodies outside the health sector. Both Alberta Health and Alberta Health Services updated a number of major system PIAs.

HIA

Alberta Health Services continues to be the largest PIA submitter under HIA, with 36 PIAs submitted and accepted. Of interest, AHS submitted a PIA for its system to manage the health services it provides to the Alberta Corrections system. Other PIAs covered systems used for laboratory services, diagnostic imaging, telehealth, paramedic services, referrals, online chronic disease management, and updates to systems that feed health information into the provincial electronic health record—Alberta Netcare.

Alberta Health submitted updates for important systems related to public health surveillance and business intelligence, as well as a PIA for the pilot Family Care Clinic.

Of the newer custodian types, both nurses and chiropractors showed a significant level of PIA compliance with 22 and 21 PIAs accepted respectively. Physicians and pharmacists continue to submit large volumes of PIAs for electronic medical record and pharmacy management systems and participation in Alberta Netcare.

FOIP

Under the FOIP Act, the PIAs of note included a PIA from Service Alberta to cover public disclosure of government officials' travel and expense information and a PIA from Alberta Health for the Seniors Property Tax Deferral Program that linked Provincial Health Numbers with income information.

Physician PIAs

2013-14 marked the end of the Physician Office System Program (POSP). Over the previous 7 years, POSP has provided PIA-writing, training and other support to physicians adopting electronic medical records. The OIPC has been able to rely on this work to establish expedited PIA review processes, allowing the Office to efficiently review over 1600 PIAs. From January-March 2014, POSP wound-up its operations and the OIPC can no longer rely on the expedited POSP PIA review processes. The OIPC expects the quality of electronic medical record PIAs to degrade over time without POSP consulting advice. Lower quality PIA submissions will mean increased OIPC review time.

To address this issue, the OIPC began offering quarterly PIA training to all sectors in 2013-14, with a special module for the health sector. Over the longer-term, the OIPC will continue to offer this training into 2014-15 and will work with stakeholders to help custodians improve their PIA submissions and seek efficiencies in PIA review at OIPC.

Investigation Reports

Student and staff personal information exposed through failure to wipe hard drives

The purchaser of a used computer server notified the OIPC that the server contained the personal information of approximately 183,900 students and 3, 500 employees of Bow Valley College.

The server was one of 21 decommissioned servers that the College had asked the Electronic Recycling Association (ERA) to pick-up. The College believed it had contracted ERA to wipe the data from the servers. However, the College had no signed contract or agreement in place with ERA, and received no written assurance that the data was wiped, or that the devices were physically destroyed.

The investigation found that the College failed to make reasonable security arrangement to protect the personal information stored on its decommissioned server, as required by the FOIP Act.

This failure resulted in the unauthorized disclosure of personal information when the server was purchased, in contravention of the FOIP Act.

The College took reasonable steps to respond to the matter, including:

- immediately ceasing to use a third party in the decommissioning of its servers;
- recovering the purchased server directly from the purchaser;
- identifying all decommissioned servers with personal information involved and contacting ERA to determine what happened to them; and
- identifying and notifying the affected individuals through a variety of means.

The College also agreed to conduct an independent audit of the controls implemented in response to the incident and to report the audit results to the OIPC.

The investigation report notes that it cost the College more than $247,900 to respond to the incident.

Bow Valley College, Investigation Report F2013-IR-01

Adjudicative body permitted to disclose police officer's name in decision posted on its website

This investigation report sets out privacy-sensitive factors adjudicative bodies should consider when posting decisions online.

A police officer's conduct was questioned during an incident, leading to a disciplinary hearing and a determination of misconduct. The officer appealed the determination to the Law Enforcement Review Board. The Board heard the appeal in public and issued a decision, which it posted on its website.

The officer complained to the OIPC that the posting of a decision that is retrievable using his name in a web search engine was a breach of his privacy.

The investigation determined that the FOIP Act permitted the Board to disclose the officer's personal information to the general public in a decision on its website. The public disclosure of the personal information was consistent with the original purposes for which the Board collected and compiled the information, i.e. conducting appeals in public. Further, the personal information in the decision was limited to the essential elements and the information was disclosed only to the extent necessary for the Board to carry out its purposes in a reasonable manner.

Law Enforcement Review Board,
Investigation Report F2013-IR-02

Project Operation Warrant Execution

The Commissioner initiated an investigation into Edmonton Police Service's program to address a large volume of outstanding warrants – Project Operation Warrant Execution (Project OWE) – to ensure that the program complied with the FOIP Act.

Project OWE was implemented in two stages. The first stage featured a public campaign that encouraged individuals to come forward and address their outstanding warrants by a certain date or risk having their names and faces advertised publicly. In the second stage, Edmonton Police Service (EPS) published names, photographs, and other personal information of individuals in various local newspapers and on the EPS website.

The investigation concluded EPS did not make reasonable security arrangements to protect personal information when it implemented Project OWE. Although EPS was authorized to disclose some personal information of individuals with outstanding warrants, EPS did not limit the extent of personal information disclosed to what was necessary to carry out its purposes in a reasonable manner. Also, EPS improperly disclosed personal information of individuals who no longer had outstanding warrants.

The investigation report recommended that EPS:

- complete and submit a Privacy Impact Assessment (PIA) to the OIPC for review prior to undertaking Project OWE again or any new initiative involving the public disclosure of personal information;
- establish a policy for requiring PIAs when designing major projects or initiatives that involve the collection, use or disclosure of personal information prior to the implementation of the project; and
- develop a review and approval process that includes the EPS FOIP Coordinator/FOIP Office in initiatives or projects that involve the collection, use or disclosure of personal information.

Edmonton Police Service,
Investigation Report F2014-IR-01

Protecting privacy with business continuity plans

Sprinklers activated by a fire in the Shaw Court building in Calgary damaged equipment and infrastructure, including servers that stored personal and health information for Service Alberta, Alberta Treasury Branches, Alberta Health, and Alberta Health Services (the respondents).

The FOIP Act, HIA, and PIPA each require that safeguards be in place to protect personal or health information against unauthorized access, loss or destruction. The Commissioner initiated an investigation into how prepared the respondents were to maintain privacy in a disaster situation.

The investigation found that three of the respondents had business continuity and disaster recovery plans in place. Alberta Health Services had components of a business continuity plan in place, but no comprehensive plan, and was therefore found to be in contravention of HIA.

Two main instances of increased risk were noted in the report:

- Having weighed the clinical risk against the privacy and security risks, Alberta Health relaxed one layer of security within its Netcare authentication system to allow users continued access during the outage; and
- Alberta Health Services reported that some staff used personal email and text messages to communicate with each other during the outage, having lost access to internal email and messaging services.

All of the respondents reported no data loss as a result of the outage. Each reviewed their actions following the outage and took steps to improve plans to prepare for similar scenarios in the future.

The investigation report makes general recommendations on business continuity planning for all public bodies, organizations and custodians in Alberta.

Service Alberta, Alberta Treasury Branches, Alberta Health, Alberta Health Services, Investigation Report F2013-IR-03/P2013-IR-01/H2013-IR-02

Pharmacist misuses health information for personal reasons

An individual complained to the OIPC that a pharmacist used her contact information from when she filled a prescription to contact her in an attempt to establish a personal relationship with her.

The pharmacist was employed on a casual basis by the pharmacy. He had access to health information for work purposes. The pharmacy resided in a retail drug store but was independently owned and operated by the pharmacy manager. The pharmacy, and not the retail drug store, was the custodian.

HIA prohibits employees from using health information for purposes other than their job responsibilities. The Act also holds a custodian responsible for the misuse of health information by its staff.

The investigation found that the pharmacist had misused health information and the pharmacy, as custodian, failed to implement reasonable safeguards to protect confidentiality, including providing privacy and security training to the pharmacist.

The pharmacy accepted the recommendation to review and follow the privacy policies and staff training requirements provided by the retail drug store. The retail drug store agreed to implement further auditing capability of its electronic information system used by the pharmacy, by logging views of records as well as logging transactions performed on a client's file.

Amani Pharmacy Ltd., Investigation Report H2013-IR-02

Clinic physicians must sign information manager agreements

One of the two physicians working at a medical clinic decided to move her practice to a new clinic. When she asked the electronic medical record (EMR) vendor to transfer records she had created while practicing at the first clinic to her new clinic, the vendor refused, stating that it had no contractual relationship with her. The physician then notified the OIPC that she believed she had lost custody and control of her records and therefore had suffered a possible privacy breach under HIA.

HIA requires physicians, as "custodians" of health information, to enter directly into agreements with information technology service providers, such as EMR vendors. These agreements are known as "information manager agreements."

The investigation revealed that the non-physician owner of the clinic had signed the agreement with the EMR vendor, rather than the physicians. Neither physician working at the clinic had signed an agreement directly with the EMR vendor, thereby contravening HIA.

Dr. Dianne Smith and Dr. Ashif Jaffer, Investigation Report H2013-IR-01

Summary of Significant Decisions

Alberta Energy ordered to refund fees on the basis of the public interest

The applicant, a representative of the Wildrose Party, requested records under the FOIP Act from Alberta Energy relating to the creation of the Critical Transmission Review Committee (CTRC) and its mandate. The applicant also made a request for records relating to the drafting of the CTRC's report entitled, "Powering Our Economy".

Alberta Energy located responsive records and required the applicant to pay fees for the records. The applicant asked to be excused from paying the fees on the basis that the records related to a matter of public interest. Alberta Energy denied the request for a fee waiver.

The Adjudicator determined that the report dealt with a matter of public interest that affected all Albertans. She also found that the applicant's purpose in obtaining the information was to generate public debate regarding the contents of the report. The Adjudicator rejected the idea that an applicant must demonstrate that the government acted inappropriately in order to qualify for a fee waiver in the public interest, as well as the argument that an applicant must establish that it intends to disseminate all the information obtained through the access request in order to establish that the information will be used to further a public interest.

The Adjudicator ordered Alberta Energy to refund the fees with regard to one access request, and to waive them with regard to the access request that it had not yet processed.

Alberta Energy, Order F2014-03

In 2013-14, the OIPC issued 74 Orders, a 68% increase from the previous fiscal year

FOIP Act and tribunals' statutory decision-making functions

Three individuals objected to the inclusion of personal information about them in an Energy Resources Conservation Board (ERCB) decision in relation to well licence review proceedings. The complainants had initiated the proceeding but then withdrawn. The decision referred to them by name, described their medical conditions, and recounted facts about various positions taken by them throughout the proceedings. The complainants also complained that a document they had provided for the hearing, which contained their personal medical information, had been made available to persons who were present in the hearing room.

The Adjudicator found that the ERCB's use and disclosure of the complainants' personal information in reaching and publishing its decision was for the same purpose for which it had been collected – to decide the issues the complainants had raised, and to present its reasons to the public in a coherent way, and that this had been done only to the extent necessary. Hence these actions of the Board were permitted under the FOIP Act. The Adjudicator commented that it is important to ensure that the restrictions in the FOIP Act are not applied to interfere inappropriately with the statutory functions of tribunals in deciding what evidence to gather, treat as relevant, and use in developing and issuing decisions. These functions should not be interfered with except in situations in which the possibility of impropriety has clearly been raised.

As to the medical information that had been made available to persons in the hearing room, the Adjudicator found the ERCB had not established that it has reasonable security arrangements in place for determining the extent to which such sensitive information should be shared with the public. She ordered the ERCB to put in place a mechanism or process that would ensure that such information would be treated appropriately.

Energy Resources Conservation Board, Order F2013-14

Alberta Human Services ordered to release certain information about children who died in care

Under the FOIP Act, a journalist asked Alberta Human Services for information about children who have died while in the care of the province. Alberta Human Services provided access to some of the requested information, but withheld other information under section 17(1) (disclosure harmful to personal privacy) and section 24(1) (advice, etc.).

The Adjudicator reviewed a sample of the approximately 1,600 pages on which information had been withheld. He found that section 17(1) applied to some of the information, as its disclosure would be an unreasonable invasion of the personal privacy of third parties, including the children. He found that section 17(1) did not apply to other information, and ordered Alberta Human Services to comply with its duty to consider all relevant circumstances in making the decision to disclose or withhold the personal information, taking note of particular guidance set out in the Order.

The Adjudicator found that Alberta Human Services had not properly applied section 24(1) to some of the information in the records, as the information was background factual information to which section 24(1) cannot apply. He therefore ordered Alberta Human Services to give the Applicant access to the background factual information. The Adjudicator found that other withheld information fell within the scope of section 24(1), as it could reasonably be expected to reveal advice, proposals, recommendations, analyses or policy options. However, he found that Alberta Human Services had not properly exercised its discretion to withhold that information. The Adjudicator therefore ordered Alberta Human Services to reconsider its decision to refuse access to the information that it had withheld under section 24(1), again taking note of particular guidance set out in the Order.

Alberta Human Services, Order F2013-19

Covenant Health ordered to disclose information about why a relative was banned from hospital premises

An individual made an access request for her personal information from Covenant Health so that she could learn the reasons for being banned from its premises and having restrictions imposed on her visiting privileges.

Covenant Health decided that section 11 of HIA applied to information about individuals other than the applicant in the records. Alternatively, it withheld this information under section 17 of the FOIP Act on the basis that the information was the personal information of individuals other than the applicant, and that it would be an unreasonable invasion of personal privacy to disclose the information. Covenant Health also subsequently applied section 24 of the FOIP Act (advice from officials) to withhold some information.

The Adjudicator determined that HIA did not apply to the information withheld by Covenant Health as it was not health information. She found that the information to which Covenant Health had applied section 17 was personal information, but that it would not be an unreasonable invasion of a third party's personal privacy to disclose it. She made this finding on the basis that the personal information was necessary for a fair determination of the applicant's rights, and because most of the personal information of the third party was about that person acting in a representative capacity.

The Adjudicator found that most of the information to which Covenant Health had applied section 24 was subject to this provision. However, she found that Covenant Health had not considered the applicant's interests in obtaining the information as part of a fair determination of her rights, when it had made the decision to withhold information under section 24. She ordered it to reconsider its decision to withhold information under section 24.

Covenant Health, Order F2013-24/H2013-02

[Covenant Health applied for judicial review of Order F2013-24/H2013-02]

Personal calls on employer-issued communication device improperly traced

An individual alleged that his employer contravened PIPA by tracing personal telephone calls that he had made using an employer-issued Blackberry device. A preliminary issue was whether the employer was subject to PIPA in the first place, given that PIPA has a limited application to a "non-profit organization", which is defined as an organization registered or incorporated under any of three specified pieces of Alberta legislation. The employer was not registered or incorporated in Alberta, but argued that it was incorporated under equivalent legislation in Ontario. Because that piece of legislation was not listed in the definition of "non-profit organization," the Adjudicator found that the employer was subject to PIPA.

The Adjudicator also found that the employer had collected and used the individual's personal information when it traced his personal calls, as the tracing revealed the recipients and the nature of the calls. The employer argued that it had collected and used the information for the purposes of an investigation under sections 14(d) and 17(d) of PIPA, further to an unwritten "acceptable use" policy regarding the Blackberry device that the employer said formed a term of the individual's employment agreement.

However, the Adjudicator found that there was, in fact, no policy in place that restricted the ability of the individual to make personal calls using the Blackberry, and there was therefore no such policy incorporated into his employment agreement. The Adjudicator therefore concluded that the employer was not authorized to collect and use the personal information revealed by the tracing of the telephone calls.

Project Porchlight, Order P2013-03

Potential for chilling effect to access rights

An applicant made an access request to Alberta Education for "all records as defined by section 1(q) of the [FOIP] Act related to communications between staff, or the minister, and [a named individual]" within a certain time frame. The applicant also requested a fee waiver, arguing that the records related to a matter of public interest, and that there were other reasons for which it was fair to waive the fees. Alberta Education refused to grant the fee waiver.

The Adjudicator determined that the records did not relate to a matter of public interest such that a fee waiver should be granted on those grounds. However, the Adjudicator determined that certain actions taken by the Minister of Education in response to the access request warranted a fee waiver in the circumstances, as the Minister had denounced the applicant for making the request, using social media. Specifically, the Minister had suggested, using a public social media platform, that the applicant had requested pictures of the Minister's children, although that was not the true purpose of the applicant's request. The Adjudicator found that these actions could create a "chilling effect" that might undermine the right of access under the FOIP Act such that the public may not feel comfortable making access requests.

The Adjudicator ordered Alberta Education to refund the fees paid by the applicant, for reasons of fairness.

Alberta Education, Order F2013-43

Employer improperly accessed personal emails

An individual complained that his former employer, Moore's Industrial Service Ltd. (Moore's) gained access to his personal web-based email account and collected, used and/or disclosed emails located in that account, in contravention of PIPA. The individual argued that his personal information was accessed without authorization, as was the personal information of former coworkers and other contacts.

The individual stated that in October 2010 he noticed that emails from his personal email account had been forwarded to Moore's CEO. The individual stated that he realized the CEO must have had access to the individual's personal email account and was forwarding some of the emails to the CEO's email account.

Moore's acknowledged that it accessed the individual's personal web-based email account, but stated that the individual had returned a work laptop that still contained his personal email account information. It argued that the individual had therefore implicitly consented to Moore's access to his personal email account.

The Adjudicator determined that the individual did not consent to Moore's to access his personal email account. She found that Moore's did not have authority to collect, use or disclose the individual's personal information contained in his email account.

Moore's Industrial Service Ltd., Order P2013-07

Judicial Reviews and Other Court Decisions

Alberta Teachers Association v. Buffalo Trail Public Schools Regional Division No. 28

2013 ABQB 283 – Judicial review of Order F2010-037

The Alberta Teachers' Association (ATA) made an access request to Buffalo Trail Public Schools Regional Division No. 28 (the Public Body) for the governing or founding documents of the School Board Employers Bargaining Authority (SBEBA) of which the Public Body was a member, and all transactional records between SBEBA and the Public Body. The Public Body withheld some of the requested information under various exceptions to disclosure contained in the FOIP Act.

The ATA requested that the Commissioner review the Public Body's decisions to withhold certain information. The ATA also requested a review of whether the Public Body complied with its duty to assist under section 10(1) of the FOIP Act, and whether it properly extended the time limit for responding to the access request, as provided by section 11(1) and section 14(1).

In an inquiry under the FOIP Act, the Adjudicator found that the Public Body had complied with its duty to assist. Furthermore, even though the Public Body was one day outside of the 30-day time limit to respond to the access request, it had made "every reasonable effort" to respond within that time and had not relied on an improper reason to extend the time. Therefore, the Adjudicator found that the Public Body had properly extended the time limit for responding to the access request.

The Adjudicator further found that section 16(1) (disclosure harmful to business interests of a third party) did not apply to allow the Public Body to withhold information from the records. Moreover, the Public Body had not properly applied section 23(1) (local public body confidences) to withhold information.

However, since the Public Body had properly applied section 25(1) (disclosure harmful to economic and other interests of a public body) and section 24(1) (advice, etc.), the Adjudicator confirmed the Public Body's decision to withhold the records from the ATA. Having made these findings, the Adjudicator did not have to consider whether the Public Body had also properly applied section 27(1) (privileged information) to withhold the records or whether section 17(1) (disclosure harmful to personal privacy) applied to the records.

The ATA applied for judicial review of Order F2010-037.

The Court held that the Adjudicator's decisions under sections 10(1), 11(1) and 14(1) were reasonable. However, the Court quashed the Adjudicator's decisions under sections 24 and 25 as being unreasonable, on the basis of a list of records that the Court said did not meet the criteria for sections 24 and section 25. The Court ordered the disclosure of SBEBA's constitution and bylaws, and remitted the section 24 and section 25 issues to the Commissioner, for a re-hearing on the issue of non-disclosure.

The Commissioner applied for reconsideration of the Court's decision, since most of the records that the Court had listed in the decision and had said did not meet the criteria for section 24 or 25 had already been disclosed by the Public Body to the ATA, and therefore the Adjudicator had not considered them. The Commissioner also requested that the Court either reconsider its decision to order disclosure of records or provide reasons for its authority to do so, since there is no disclosure remedy available on a judicial review application. Furthermore, the Adjudicator had not yet considered whether section 17 and section 27(1) applied to the records the Court ordered disclosed.

The Court issued a correction to the decision to delete all but one item in the records listed as not meeting the criteria for section 24 and section 25. The Court did not provide reasons for the disclosure order and did not reconsider the disclosure order.

The Commissioner has appealed the Court's decision to order disclosure of records.

Imperial Oil Limited v. Calgary (City)

2013 ABQB 393 – Judicial review of Order F2005-030

The City of Calgary (the City) made an access request to Alberta Environment (the Public Body) for a remediation agreement between the Public Body and Imperial Oil, relating to the cleanup of land in Calgary that had been contaminated by hydrocarbon vapours and lead. The Public Body and Imperial Oil released some information about the agreement through press releases and released some parts of the agreement to the City, with conditions against further disclosure. However, the Public Body refused to release the entire agreement in response to the access request, claiming that a number of exceptions to disclosure under the FOIP Act applied: section 16 (disclosure harmful to business interests of a third party), section 17 (disclosure harmful to personal privacy), section 24 (advice, etc.), section 25 (disclosure harmful to economic and other interests of a public body), and section 27 (settlement negotiation privilege). The City asked the Commissioner to review the Public Body's decision.

In an inquiry under the FOIP Act, the Commissioner found that, with the exception of personal information of third parties withheld under section 17 and a small amount of information withheld under section 16, none of the exceptions to disclosure applied. He ordered disclosure of the entire agreement, other than the information mentioned above. The City had argued that section 32 (disclosure in the public interest) should apply. However, since the Commissioner had decided to order disclosure of the agreement, he found that he did not need to consider section 32, except for the information he ordered not to be disclosed, for which he held that section 32 did not apply.

Imperial Oil Limited, a third party in the inquiry, applied for judicial review of Order F2005-030.

The Court found that the following standards of review applied to the Commissioner's decisions:

- section 16(1)(a)(i): information of a third party – reasonableness;
- section 16(1)(b): information supplied explicitly or implicitly in confidence – reasonableness;
- section 16(1)(c): harm – standard of review not decided;
- section 16(3)(b): enactment of Alberta or Canada authorizing or requiring disclosure – correctness;
- section 24(1): advice, etc. – reasonableness;
- section 25(1): harm to economic or other interests of public body – reasonableness; and
- sections 27(1)(a), (2): privileged information – correctness.

The Court held that the Commissioner's decisions under sections 16, 24, 25 and 27 were either unreasonable or incorrect. The Court quashed Order F2005-030.

The Commissioner has appealed the Court's decision.

University of Calgary v. JR

2013 ABQB 652 – Judicial review of an Adjudicator's Notice to Produce Records alleged to be subject to solicitor – client privilege

An individual, a former employee of the University of Calgary (the Public Body), made an access request for information held by various other employees of the Public Body, a Wellness Centre and a doctor associated with the Wellness Centre. The Public Body provided some of the information, but withheld other information under various exceptions to disclosure contained in the FOIP Act, including section 27(1)(a) (solicitor – client privilege). The individual requested that the Commissioner review the Public Body's decisions to withhold information.

In an inquiry under the FOIP Act, the Public Body chose not to provide the Adjudicator with a copy of the records for which it claimed that solicitor – client privilege applied, in accordance with the Solicitor – client Privilege Adjudication Protocol of the Commissioner's Office. In accordance with the Protocol, the Adjudicator requested additional argument and evidence from the Public Body so that he could decide whether it properly applied section 27(1)(a) to the records. The Public Body provided a minimal amount of additional information, which was insufficient for the Adjudicator to decide the issue. The Adjudicator sent the Public Body a notice under section 56(2) of the FOIP Act to produce the records so that he could decide whether the Public Body had the authority to withhold those records.

The Public Body applied for judicial review of the Adjudicator's Notice to Produce Records.

The Court held that the standard of review was correctness, and that the FOIP Act gave the Adjudicator authority to issue a Notice to Produce in relation to records alleged to be subject to solicitor – client privilege. The Court also held that recourse to the Notice to Produce was necessary in this case to verify the claim for privilege. The Court upheld the Adjudicator's decisions as being correct.

The University of Calgary has appealed the Court's decision.

Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401

2013 SCC 62, which upheld, except as to remedy, 2012 ABCA 130, which upheld, except as to remedy, 2011 ABQB 415, which partially quashed Order P2008-008 on constitutional grounds

The Court of Queen's Bench partially quashed Order P2008-008, on the grounds that section 4(3)(c) of PIPA and section 7 of the PIPA Regulation violated the Union's freedom of speech under section 2(b) of the *Canadian Charter of Rights and Freedoms* (the Charter).

The Attorney General of Alberta appealed the decision of the Court of Queen's Bench. The Court of Appeal held that:

- the infringement of the Union's right to free expression under section 2(b) of the Charter, arising from PIPA, could not be justified under the tests set out in *R. v. Oakes*;

- the Adjudicator's decision was unreasonable because its effect on the Union's expressive rights was disproportionate; and
- it was within the mandate of the Legislature to decide what amendments were required to PIPA in order to bring it in line with the Charter.

Rather than declare that parts of PIPA were unconstitutional, the Court of Appeal issued a declaration that the application of PIPA to the Union's activities was unconstitutional.

The Information and Privacy Commissioner and the Attorney General of Alberta appealed to the Supreme Court of Canada. The Supreme Court held that:

- PIPA's purpose is to provide an individual with control over the collection, use and disclosure of the individual's personal information, without consent;
- PIPA does not include any mechanisms by which a union's constitutional right to freedom of expression on the picket line may be balanced with the interests PIPA protects; and
- The infringement of the right to freedom of expression is disproportionate to the objective of providing individuals with control over their personal information, and cannot be justified under section 1 of the Charter.

Rather than deciding which parts of PIPA were unconstitutional, the Supreme Court followed the recommendation of the Information and Privacy Commissioner and the Attorney General of Alberta and declared the entirety of PIPA to be unconstitutional. The Supreme Court suspended its declaration of unconstitutionality for one year to give the Alberta Legislature time to redraft PIPA so that it would be constitutionally compliant.

On the basis that PIPA was unconstitutional, the Supreme Court quashed Order P2008-008.

Workers Compensation Board v. Alberta (Information and Privacy Commissioner)

2014 ABQB 99 – Judicial review of Order F2013-11

An individual made an access request to the Workers' Compensation Board (the Public Body) for records relating to his claim, and then requested that the Public Body reopen his claim. He provided a medical opinion from his physician to support his request to reopen.

The Public Body sent the medical opinion by regular mail to the Appeals Commission for Alberta Workers' Compensation (the Appeals Commission), along with a covering letter addressed "To Whom it May Concern." The Appeals Commission had no record of receiving the medical opinion.

The Public Body also sent the covering letter to the individual and to a consulting company that the Public Body believed, in error, represented the individual.

The individual complained to the Commissioner that the Public Body disclosed his personal information to the consulting company and sent his medical information to the Appeals Commission, without authority and contrary to the FOIP Act. He also asked the Commissioner to review whether the Public Body had made every reasonable effort to ensure that his personal information was accurate and complete, as required by section 35(a) of the FOIP Act, and whether the Public Body had made reasonable security arrangements to protect his personal information, as required by section 38 of the FOIP Act. He further asked the Commissioner to review the Public Body's response to his access request, on the basis that records were missing.

In an inquiry under the FOIP Act, the Adjudicator found that the Public Body had (1) met its duty to assist the individual, as required by section 10(1) of the FOIP Act; (2) not contravened section 35 of the FOIP Act when it referred the individual's request and medical opinion to the Appeals Commission; (3) contravened section 38 of the FOIP Act when it sent the individual's personal information to the consulting company, without confirming whether the consulting company was authorized to receive the individual's personal information; and (4) contravened section 38 of the FOIP Act by sending the medical opinion to the Appeals Commission by regular mail and by failing to specify an authorized addressee. In finding that the Public Body contravened section 38 of the FOIP Act, the Adjudicator interpreted provisions of the *Workers' Compensation Act*.

The Adjudicator ordered the Public Body to ensure that all correspondence containing the individual's personal information was sent and addressed only to those authorized to receive it, and sent by secure, traceable means.

The Public Body applied for judicial review of Order F2013-11.

The Court held that the reasonableness standard of review applied. Although the Court was of the view that the *Workers' Compensation Act* was not closely connected to the OIPC's function, the Court said that, given the OIPC's broad mandate, the OIPC would necessarily consider other statutes in order to determine whether the FOIP Act had been breached.

The Court held that the Adjudicator's order was reasonable except for that part of the order requiring health information to be sent by the Public Body by secure, traceable means, which the Court found was unreasonable to the extent that this precluded regular prepaid mail in cases where registered mail was not expressly required by statute.

Peter Choate and Associates Ltd. v. Dahlseide

2014 ABQB 117 – Judicial review of Order P2012-05

Two individuals complained that their personal information had been improperly disclosed by Peter Choate and Associates Ltd. (the Organization) to a third party while they were attending counselling sessions. The Organization argued that some of the information was not personal information. Further, the Organization argued that information that was personal information had been used or disclosed for the purpose of a legal proceeding or under the *Family Law Act*, and that use or disclosure was therefore authorized without consent under PIPA.

The Organization relied on section 4(5)(a) of PIPA as not limiting the information available by law to a party to a legal proceeding. The Adjudicator also considered whether section 4(3)(k) of PIPA (personal information in a court file) operated to exclude the application of PIPA.

In an inquiry under PIPA, the Adjudicator found that:

- the Organization had fulfilled its obligation to have privacy policies and practices;
- section 4(3)(k) did not apply because the personal information was not in a court file at the time of the disclosure;
- the purpose of section 4(5)(b) was to ensure that the restrictions in PIPA were not interpreted so as to interfere with or override a statutory or common law process that made information available to a party to a proceeding. However, personal information in the possession of an organization that may be related to a proceeding was not "available by law" to the organization or anyone else to whom the organization chose to disclose the information, simply by virtue of the fact that there was a legal proceeding to which the information may relate;
- all the information at issue was personal information;
- the individuals were deemed to have consented to the collection of the personal information, but not to the use or disclosure; and

- the *Family Law Act* authorized the disclosure of only some of the personal information of one individual, but the Organization did not have authority to use and disclose the remaining personal information of that individual or any personal information of the other individual.

The Adjudicator ordered the Organization to stop using and disclosing the personal information for which it lacked authority.

The Organization applied for judicial review of those parts of Order P2012-05 in which the Adjudicator did not find in the Organization's favour.

The Court held that the reasonableness standard of review applied to the Adjudicator's interpretation of section 4(3)(k) and section 4(5)(b) of PIPA because the Adjudicator was interpreting her home statute. The Court held that the Adjudicator was both correct and reasonable in her interpretations.

The Court held that the reasonableness standard of review also applied to the Adjudicator's interpretation that the definition of personal information included an opinion that revealed what an identified individual valued. The Court held that the Adjudicator's decision was reasonable as it met the requirements of justification, transparency and intelligibility, and fell within a range of possible acceptable outcomes that were defensible in respect of the facts and the law.

The Court further held that the reasonableness standard of review applied to the Adjudicator's interpretations of provisions of the *Family Law Act*, on the basis that the privative clause and nature of the questions (mixed fact and law) supported the reasonableness standard for the interpretation of one provision, and on the basis that the strong privative language in PIPA, the policy aspects engaged by the question and the purpose of the tribunal supported the reasonableness standard for the interpretation of another provision. Furthermore, taking into consideration that the Organization failed to provide evidence, the Court held that the Adjudicator was reasonable in her interpretations.

Finally, the Court held that the reasonableness standard of review applied to the Adjudicator's balancing of the competing interests involved under PIPA, since the policy choices were delegated to the Commissioner to decide and not to the Court to decide on review. The Court's view was that the Adjudicator's balancing was not unreasonable.

The Court denied the application for judicial review.

Calgary Board of Education v. Alberta (Office of the Information and Privacy Commissioner)

2014 ABQB 189 – Judicial review of Order F2009-048

An individual who was a former employee of the Calgary Board of Education (the Public Body) gave evidence as a witness in a Board of Reference (Board) proceeding involving another employee of the Public Body. The Public Body sought to introduce documents that related to incidents involving the individual, which had occurred several years earlier and which were not related to the Board proceeding. After the Public Body disclosed some of the information to the Board, the Board ordered the Public Body to disclose the documents to the Board and to the other party in the proceeding, so that the Board could decide whether to admit the information as evidence. After reviewing the documents, the Board decided not to admit them into evidence.

The individual complained to the Commissioner that the Public Body had used and disclosed his personal information, contrary to the FOIP Act, and had not made reasonable security arrangements to protect his personal information.

In an inquiry under the FOIP Act, the Adjudicator decided that the Public Body's use and initial disclosure of the personal information to the Board was not authorized under the FOIP Act and therefore contravened the FOIP Act. However, the subsequent disclosure of the personal information for the purpose of complying with the Board's order was authorized. The Adjudicator also found that the Public Body had not failed in its duty to protect the individual's personal information.

The Public Body applied for judicial review of that part of Order F2009-048 in which the Adjudicator had found that the Public Body contravened the FOIP Act.

In the judicial review, the Public Body argued that the Adjudicator was interpreting the *School Act* and the *Public Inquiries Act*, which was legislation that was outside her home statute and over which she had no expertise. The Public Body therefore argued that the standard of review for the Adjudicator's decision should be correctness, rather than reasonableness.

The Court was of the view that merely because the questions before the Adjudicator required her to consider other statutes did not bring the matter outside of the FOIP Act or the Adjudicator's specialized area of expertise. The role of the Commissioner under section 2(b) of the FOIP Act (controlling the manner in which a public body may collect, use and disclose personal information) meant that the Commissioner would necessarily have to interpret the relationship between other statutes and the FOIP Act. Given the nature of the Commissioner under the FOIP Act, the Adjudicator's role in determining FOIP issues in relation to various public bodies with unique legislative schemes, and the presumption of reasonableness, the Court found that the Adjudicator's decision was within her area of expertise.

The Court said that the Adjudicator's decision that the Public Body used and disclosed the individual's information was reached after thorough review of the relevant legislation, facts and policy. The Adjudicator's reasons were justifiable, transparent and intelligible, and the decision she reached was within the range of possible, acceptable outcomes that were defensible on the relevant law and facts. Therefore, the Court found that the Adjudicator's decision was reasonable, and upheld the decision.

Education & Outreach

The mandate of the OIPC includes a strong commitment to education and outreach. From publications to presentations and consultations, the Office continues to raise public awareness of the access to information and privacy rights under the FOIP Act, HIA and PIPA, provide guidance and direction to stakeholders to enhance compliance, and facilitate opportunities for the public and stakeholders to comment on the administration of the Acts, OIPC processes, and access and privacy issues in general.

The following are highlights of the informational and educational activities undertaken by the OIPC in 2013-14.

Presentations, Forums and Workshops

In 2013-14, the Commissioner and OIPC staff participated in 73 presentations and speaking engagements, provincially and nationally. These events generally focused on emerging trends and issues in access and privacy, and the application of the FOIP Act, HIA and PIPA.

Educating young Albertans about access to information and privacy continued to be a priority, with the Office participating monthly in the Legislative Assembly of Alberta's School at the Legislature program.

The OIPC also continued its support of the University of Alberta's annual Access and Privacy Conference, participating on the Conference Advisory Committee, conducting a workshop on cross-sectoral privacy impact assessments (PIAs), and holding an informal "Open Dialogue" with the Commissioner and senior staff of the OIPC.

The following highlight some other key presentations, forums and workshops from 2013-14.

Accountability Project Phase V Spring Meeting

In May 2013, the Commissioner presented at the Accountability Project Phase V Spring Meeting in Toronto, facilitated by The Centre for Information Policy Leadership and the Office of the Privacy Commissioner of Canada. The Accountability Project is an international, multi-stakeholder initiative for which the Centre serves as secretariat. A significant part of the agenda for the meeting in May was focused on the joint guidance developed by the Office of the Privacy Commissioner of Canada and the Alberta and BC OIPCs on *Getting Accountability Right with a Privacy Management Program*. Attendees at the meeting included representatives from international organizations and data protection authorities.

Western Canada Health Information Privacy Symposium (WCHIPS)

The second annual Western Canada Health Information Privacy Symposium (WCHIPS) was held in May 2013 in Winnipeg, Manitoba. The 2013-14 event, which was co-hosted by the Manitoba Ombudsman and the Information and Privacy Commissioners of Alberta, Saskatchewan and British Columbia, was focused on "Meeting the Challenge of Stewarding Health Information" and gave participants from the four western provinces an opportunity to network and learn about how to successfully address common privacy problems and challenges.

The agenda featured presentations on privacy breach response, health research, employee health information, the use of auditing technology to detect misuse of health information, and electronic health records.

Right to Know 2013

Right to Know Week is an annual global event to raise awareness of an individual's right to access government information while promoting freedom of information as essential to democracy and good governance.

In recognition of Right to Know 2013, the Commissioner hosted one-day "Shining the Spotlight on Access" forums in Edmonton and Calgary. The forums featured presentations focused on making information more accessible, including:

- Brent Rathgeber, independent Member of Parliament for Edmonton-St. Albert, speaking about federal access to information and sunshine laws, transparency and openness;
- Lorna Stefanick, author of *Controlling Knowledge: Freedom of Information and Protection of Privacy in a Networked World;*

- Barbara Carra, Cybera, offering insight into the infrastructure requirements of making information available electronically;
- Cathryn Landreth and Mark Diner, Service Alberta, on the Government of Alberta's Open Data Portal; and
- Tom Seaman, City of Calgary, on challenges to access to information during the southern Alberta floods.

Hacking Health Edmonton

In November 2013, the OIPC participated in Hacking Health Edmonton, an event designed to bring together small teams of healthcare professionals, computer programmers, graphic designers and others to create IT solutions to healthcare problems (e.g. a secure way to refer patients within the health system, an app that helps parents to record their children while they are displaying symptoms). Staff of the OIPC participated as an access and privacy mentor for the event.

Respectful Information Sharing Day

Also in November, senior OIPC staff members presented to representatives of 13 First Nations communities involved in primary care projects as part of the "Respectful Information Sharing Day". The purpose of the Respectful Information Sharing Day was to understand relationships, roles and guidelines around health information and privacy in Alberta. The session was part of a project supported by the Health Services Integration Fund (HSIF), a five-year initiative supporting collaborative planning and multi-year projects aimed at better meeting the health-care needs of First Nations and Inuit. The OIPC presentation focused on common themes from discussions with First Nations under HIA, including concepts of ownership, custody and control of health information; employment relationships; transferring records to successor custodians; and, Netcare access.

The Ins and Outs of Alberta's Privacy Legislation REACH Edmonton

Information sharing across sectors is an increasingly important issue and the OIPC welcomes opportunities to address a diverse group of human services organizations about this topic. In November 2013, REACH Edmonton, a community-based non-profit organization, facilitated a half-day event for community groups, agencies and organizations, and senior OIPC staff to talk about Alberta's privacy legislation and information sharing between service providers for the purpose of enhancing client outcomes. The discussion focused on the application of Alberta's privacy laws, the extent to which they authorize or facilitate information sharing, and some of the challenges—including the perception that privacy laws are a barrier to information sharing. As this topic comes increasingly to the forefront, events such as this one are essential for opening dialogue and raising awareness for all stakeholders.

Data Privacy Day

Held annually on January 28, Data Privacy Day is recognized by privacy professionals, corporations, government officials, academics and students around the world. It highlights the impact that technology is having on our privacy rights and aims to educate and empower people to value and protect personal information.

To celebrate Data Privacy Day, the Commissioner hosted a full-day forum in Edmonton featuring presentations on privacy best practices, emerging trends in surveillance and cyberbullying, and a retrospective panel discussion on ten years of private sector privacy legislation in Alberta.

PIA Workshops

Part of the OIPC's 2013-14 education and outreach plan entailed focusing resources on holding a few issue-specific workshops and seminars, rather than hosting larger legislation-specific conferences. To this end, in February 2014, the OIPC hosted Privacy Impact Assessment (PIA) training workshops in both Calgary and Edmonton.

Completing a PIA is a due diligence exercise in which a custodian, public body or organization identifies and addresses potential privacy risks that may occur in the course of its operations or when implementing a new or changed information system or program. PIAs are mandatory under Alberta's HIA and are recommended for major projects that involve the collection, use or disclosure of personal information under the FOIP Act or PIPA.

Each full-day training session featured PIA Essentials for all sectors in the morning, followed by a PIA Advanced Development seminar for the health sector in the afternoon.

These 'sold-out' workshops were attended by professionals responsible for completing PIAs on behalf of physicians, nurses, chiropractors, midwives, dentists, dental hygienists, pharmacists, clinic managers, FOIP coordinators, and privacy officers.

Given the popularity of these workshops, the OIPC has committed to repeating them throughout 2014-15.

Collaboration with Other Jurisdictions

The OIPC collaborates with the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner for British Columbia, and the other provincial and territorial privacy oversight offices to develop educational publications and information pieces for stakeholders.

Privacy Emergency Kit

Privacy laws should not be a barrier to appropriate information sharing in disaster or emergency situations; however, it is important that first responders, health custodians, government workers, organizations and citizens know how personal or health information may be shared in such situations.

In 2013-14, the Alberta OIPC worked with the Office of the Privacy Commissioner of Canada and other Canadian provincial and territorial privacy oversight offices to publish a guidance document to help organizations enhance the timeliness and content of communications during an emergency while giving people confidence that their personal information will be handled appropriately.

Data Protection Authorities raise questions about Google Glass

In June 2013, the Alberta Information and Privacy Commissioner, along with other Canadian and international oversight offices, wrote to Google Inc. to raise concerns about the privacy implications of Google Glass, a type of computing technology that can be worn by an individual and used to film and record audio of other people. The letter asked a number of questions about how Google Glass complies with data protection laws, including implementing privacy safeguards, what information Google collects via Glass, and what information is shared with third parties such as application developers. All signatories to the joint letter expressed willingness to meet with Google Inc. to discuss the privacy issues raised by Google Glass.

Canada's access to information and privacy guardians urge government to modernize laws

In October 2013, the Information and Privacy Commissioners and Ombudspersons from federal, provincial and territorial jurisdictions across Canada issued a joint resolution calling on governments to update access to information and privacy laws. In advocating for modern, effective laws, the resolution noted heightened citizen concerns in the face of revelations about government surveillance programs, as well as increased calls for government transparency. The resolution set out a number of possible reforms for consideration, including:

- mandatory breach reporting and notification of affected individuals;
- legislating a duty to document the deliberations, actions and decisions of public entities; and
- strong monitoring and enforcement powers for regulators.

Media Enquiries

The OIPC responded to 117 media enquiries during 2013-14. The issues receiving significant media attention included:

- The Commissioner's comments on concerns with Bill 25, the *Children First Act;*
- Government of Alberta severance packages and proactive disclosure of salary information;
- The Supreme Court of Canada decision which ruled PIPA unconstitutional for infringing on the Charter rights of the United Food and Commercial Workers in relation to picketing activity;
- OIPC's release of its investigation report on the Shaw Court Building fire in Calgary, which affected computer systems holding personal, health and financial information of Albertans;
- Government of Alberta publication ban on the disclosure of names of children in care;
- Medicentres' privacy breach concerning the loss of an unencrypted laptop containing health information; and
- OIPC's release of its investigation report on the Edmonton Police Service's outstanding warrant initiative, known as Project OWE.

Robert C. Clark Award

In late 2012, the Information and Privacy Commissioner announced the creation of the Robert C. Clark Award to recognize an individual, group or public body who has contributed significantly to advancing access to information in Alberta.

The annual award is named after Alberta's first Information and Privacy Commissioner, Robert (Bob) Clark, who served in the role from 1995 to 2001. Clark led the Office through the introduction and expansion of the FOIP Act, and the introduction of HIA, while also acting as an educator and advocate for the principles of access to information and protection of privacy.

The first recipient of the Robert C. Clark Award, Mr. Wayne MacDonald, was announced in September 2013 during Right to Know Week.

Mr. MacDonald is the Government Studies Program Manager with the Faculty of Extension at the University of Alberta and has played a significant role in the education of information rights administrators in the province of Alberta and across Canada.

A dedicated leader and champion in the area of access rights, Mr. MacDonald was integral in the development of the Information Access and Protection of Privacy (IAPP) Certificate Program at the University of Alberta. The IAPP program has an annual registration of 450 students and has received national and international recognition as the leading post-secondary program supporting information rights legislation and administration.

As well, Mr. MacDonald chairs the highly-regarded, annual access and privacy conference, and developed an IAPP awards recognition program and specialized information access training for governments.

The recipient of the award is determined by an independent, three-person panel made up of subject matter experts with extensive experience in the field. The 2013 panel members were:

- Irene Hamilton, former Ombudsman for the province of Manitoba;
- Elaine Keenan Bengts, Information and Privacy Commissioner of the Northwest Territories; and
- Laura Neuman, Senior Associate Director of the Americas Program, and Manager of the Global Access to Information Initiative with the Carter Center in Atlanta, Georgia.

Financial Statements

Independent Auditor's Report 56
Statement of Operations 57
Statement of Financial Position 58
Statement of Cash Flows 59
Notes to the Financial Statements 60
Schedule 1 – Salary and Benefits Disclosure 65
Schedule 2 – Allocated Costs 66

AUDITOR GENERAL *Alberta*

Independent Auditor's Report

To the Members of the Legislative Assembly:

Report on the Financial Statements

I have audited the accompanying financial statements of the Office of the Information and Privacy Commissioner, which comprise the statement of financial position as at March 31, 2014, and the statements of operations and cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with Canadian public sector accounting standards, and for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with Canadian generally accepted auditing standards. Those standards require that I comply with ethical requirements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Opinion

In my opinion, the financial statements present fairly, in all material respects, the financial position of the Office of the Information and Privacy Commissioner as at March 31, 2014, and the results of its operations, its remeasurement gains and losses, and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

Original signed by
Merwan N. Saher, FCA

Auditor General
June 17, 2014
Edmonton, Alberta

Office of the Information and Privacy Commissioner

Statement of Operations

Year ended March 31, 2014

	2014 Budget	2014 Actual	2013 Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 4,775	$ 22,972
Other Revenue	-	567	1,206
	-	5,342	24,178
Expenses – Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 5,535,000	$ 4,781,805	$ 5,030,618
Supplies and Services	1,222,000	1,293,633	1,136,345
Amortization of Tangible Capital Assets	64,000	56,556	55,550
Total Expenses	6,821,000	6,131,994	6,222,513
Net Operating Results	$ (6,821,000)	$ (6,126,652)	$ (6,198,335)

The accompanying notes and schedules are part of these financial statements.

Financial Statements

Office of the Information and Privacy Commissioner

Statement of Financial Position

As at March 31, 2014

	2014	2013
Assets		
Cash	$ 100	$ 100
Accounts Receivable	34	3,187
Prepaid Expenses	905	765
Tangible Capital Assets (Note 4)	267,745	176,107
	$ 268,784	$ 180,159
Liabilities		
Accounts Payable and Accrued Liabilities	$ 461,701	$ 222,831
Accrued Vacation Pay	479,201	446,585
	940,902	669,416
Net Liabilities		
Net Liabilities at Beginning of Year	(489,256)	(303,850)
Net Operating Results	(6,126,652)	(6,198,335)
Net Financing Provided from General Revenues	5,943,790	6,012,928
	(672,118)	(489,257)
	$ 268,784	$ 180,159

The accompanying notes and schedules are part of these financial statements.

Office of the Information and Privacy Commissioner

Statement of Cash Flows

Year ended March 31, 2014

	2014	2013
Operating Transactions		
Net Operating Results	$ (6,126,652)	$ (6,198,335)
Non-cash Items Included in Net Operating Results		
Amortization of Tangible Capital Assets	56,556	55,550
Loss on Disposal of Tangible Capital Assets	-	1,260
	(6,070,096)	(6,141,525)
(Increase) Decrease in Accounts Receivable	3,153	(3,142)
Decrease (Increase) in Prepaid Expenses	(140)	6,745
Increase (Decrease) in Accounts Payable	271,486	140,858
Cash Applied to Operating Transactions	(5,795,597)	(5,997,064)
Capital Transactions		
Acquisition of Tangible Capital Assets	(148,193)	(15,864)
Financing Transactions		
Net Financing Provided From General Revenues	5,943,790	6,012,928
Cash, Increase (Decrease)	-	-
Cash, Beginning of Year	100	100
Cash, End of Year	$ 100	$ 100

The accompanying notes and schedules are part of these financial statements.

Financial Statements

Office of the Information and Privacy Commissioner

Notes to the Financial Statements

Year ended March 31, 2014

Note 1 Authority

The Office of the Information and Privacy Commissioner operates under the authority of the *Freedom of Information and Protection of Privacy Act*. The net cost of the operations of the Office is borne by the General Revenue Fund of the Province of Alberta. Annual operating budgets are approved by the Standing Committee on Legislative Offices.

Note 2 Purpose

The Office of the Information and Privacy Commissioner provides oversight on the following legislation governing access to information and protection of privacy:

Freedom of Information and Protection of Privacy Act
Health Information Act
Personal Information Protection Act

The major operational purposes of the Office of the Information and Privacy Commissioner are:

- To provide independent reviews of decisions made by public bodies, custodians and organizations under the Acts and the resolution of complaints under the Acts;
- To advocate protection of privacy for Albertans; and
- To promote openness and accountability for public bodies.

Note 3 Summary of Significant Accounting Policies and Reporting Practices

These financial statements are prepared in accordance with Canadian Public Sector Accounting Standards.

a) Reporting Entity

The reporting entity is the Office of the Information and Privacy Commissioner (the Office), for which the Information and Privacy Commissioner is responsible.

The Office operates within the General Revenue Fund (the Fund). The Fund is administered by the President of Treasury Board and Minister of Finance. All cash receipts of the Office are deposited into the Fund and all cash disbursements made by the Office are paid from the Fund. Net Financing provided from General Revenues is the difference between all cash receipts and all cash disbursements made.

b) Basis of Financial Reporting

Revenues

All revenues are reported on the accrual basis of accounting.

Expenses

Directly Incurred

Directly incurred expenses are those costs the Office has primary responsibility and accountability for, as reflected in the Office's budget documents.

In addition to program operating expenses such as salaries, supplies, etc., directly incurred expenses also include:

- Amortization of tangible capital assets;
- Pension costs, which are the cost of employer contributions for current service of employees during the year; and
- Valuation adjustments which represent the change in management's estimate of future payments arising from obligations relating to vacation pay.

Incurred by Others

Services contributed by other entities in support of the Office's operations are not recognized and are disclosed in Schedule 2.

Assets

Financial assets are assets that could be used to discharge existing liabilities or finance future operations and are not for consumption in the normal course of operations. Financial assets of the Office are limited to financial claims, such as receivables from other organizations.

Tangible capital assets of the Office are recorded at historical cost and are amortized on a straight-line basis over the estimated useful lives of the assets. The threshold for tangible capital assets is $5,000.

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2014

Liabilities

Liabilities are recorded to the extent that they represent present obligations as a result of events and transactions occurring prior to the end of the fiscal year. The settlement of liabilities will result in sacrifice of economic benefits in the future.

Net Liabilities

Net liabilities represent the difference between the Office's liabilities and the carrying value of its assets.

Canadian Public Sector Accounting Standards require a "net debt" presentation for the statement of financial position in the summary financial statements of governments. Net debt presentation reports the difference between financial assets and liabilities as "net debt" or "net financial assets" as an indicator of the future revenues required to pay for past transactions and events. The Office operates within the government reporting entity, and does not finance all its expenditures by independently raising revenues. Accordingly, these financial statements do not report a net debt indicator.

Valuation of Financial Assets and Liabilities

Fair value is the amount of consideration agreed upon in an arm's length transaction between knowledgeable, willing parties who are under no compulsion to act.

The fair values of Cash, Accounts Receivable, Accounts Payable and Accrued Liabilities are estimated to approximate their carrying values because of the short term nature of these instruments.

c) Financial Instruments

As the Office does not have any transactions involving financial instruments that are classified in the fair value category and has insignificant foreign currency transactions, there are no remeasurement gains and losses and therefore a statement of remeasurement gains and losses has not been presented.

Notes to the Financial Statements *(continued)*

Year ended March 31, 2014

Note 4 Tangible Capital Assets

	Office equipment and furniture	Computer hardware and software	Total
Estimated Useful Life	10 years	3-5 years	
Historical Cost			
Beginning of Year	$ 236,729	$ 279,880	$ 516,609
Additions	-	148,193	148,193
Disposals, Including Write-Downs	-	(14,138)	(14,138)
	$ 236,729	$ 413,935	$ 650,664
Accumulated Amortization			
Beginning of Year	$ 190,767	$ 149,735	$ 340,502
Amortization Expense	13,025	43,531	56,556
Effect of Disposals	-	(14,139)	(14,139)
	$ 203,792	$ 179,127	$ 382,920
Net Book Value at March 31, 2014	$ 32,937	$ 234,808	$ 267,745
Net Book Value at March 31, 2013	$ 45,962	$ 130,145	$ 176,107

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2014

Note 5 Defined Benefit Plans

The Office participates in the multiemployer pension plans: Management Employees Pension Plan, Public Service Pension Plan and Supplementary Retirement Plan for Public Service Managers. The expense for these pension plans is equivalent to the annual contributions of $601,047 for the year ended March 31, 2014 (2013 - $629,547).

At December 31, 2013, the Management Employees Pension Plan reported a deficiency of $50,457,000 (2012 - deficiency $303,423,000) and the Public Service Pension Plan reported a deficiency of $1,254,678,000 (2012 - deficiency $1,645,141,000). At December 31, 2013, the Supplementary Retirement Plan for Public Service Managers had a deficiency of $12,384,000 (2012 - deficiency $51,870,000).

The Office also participates in a multiemployer Long Term Disability Income Continuance Plan. At March 31, 2014, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $24,055,000 (2013 - surplus $18,327,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 6 Contractual Obligations

Contractual obligations are obligations of the Office to others that will become liabilities in the future when the terms of those contracts or agreements are met.

	2014	2013
Obligations under operating leases and contracts	$ 26,356	$ 24,989

Estimated payment requirements for each of the next three years are as follows:

	Total
2014-15	$ 20,395
2015-16	5,961
2016-17	-
	$ 26,356

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Note 7 Comparative Figures

Certain 2013 figures have been reclassified to conform to the 2014 presentation.

Note 8 Approval of Financial Statements

These financial statements were approved by the Information and Privacy Commissioner.

Salary and Benefits Disclosure

Schedule 1

Year ended March 31, 2014

	2014				2013
	Base Salary [a]	Other Cash Benefits [b]	Other Non-cash Benefits [c][d]	Total	Total
Senior Official					
Information and Privacy Commissioner [d]	$ 197,672	$ 1,850	$ 69,174	$ 268,696	$ 251,293

[a] Base salary includes pensionable base pay.
[b] Other cash benefits include vacation payouts and lump sum payments. A lump sum payment of $1,850 per employee was approved by the union respecting 2014.
[c] Other non-cash benefits include the government's share of all employee benefits and contributions or payments made on behalf of employee, including pension, supplementary retirement plan, health care, dental coverage, group life insurance, short and long term disability plans, health spending account, conference fees, and professional memberships and tuition fees.
[d] Automobile provided. Taxable benefit amount included in other non-cash benefits.

Office of the Information and Privacy Commissioner

Schedule 2

Allocated Costs

Year ended March 31, 2014

	2014				2013
	Expenses - Incurred by Others				
Program	Expenses [a]	Accommodation Costs [b]	Telephone Costs [c]	Total Expenses	Total Expenses
Operations	$ 6,131,994	$ 446,655	$ 15,707	$ 6,594,356	$ 6,679,566

[a] Expenses - Directly Incurred as per Statement of Operations.
[b] Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.
[c] Telephone Costs is the line charge for all phone numbers.

Appendices

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type 68

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type 71

Appendix C: Orders, Decisions and Public Investigation Reports Issued 74

Appendix D: Accepted Privacy Impact Assessments by Public Body and Custodian Types 77

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period April 1, 2013 to March 31, 2014

FOIP Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Disclosure to Commissioner	Authorization to Indirectly Collect	Total
Agencies	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
Boards	0	0	4	1	0	1	1	0	0	2	4	1	2	1	0	0	17
Child and Family Service Authorities	0	0	2	0	0	0	0	0	0	0	2	0	4	0	0	0	8
Colleges	0	0	2	0	0	0	0	0	0	0	3	0	0	1	0	0	6
Commissions	0	0	1	0	0	2	0	0	0	0	9	1	2	1	0	0	16
Committees	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Crown Corporations	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	2
Federal Departments	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Foundation	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Government Ministries/ Departments	1	0	52	1	0	4	4	0	9	14	138	7	62	3	1	1	297
Hospital Board (Covenant Health)	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	2
Law Enforcement Agencies	0	0	9	2	0	1	0	0	0	1	38	0	0	0	0	0	51
Legislative Assembly Offices	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Local Government Bodies	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	0	4
Long Term Care Centres	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Municipalities	0	0	7	0	0	16	0	0	3	1	28	11	9	4	0	0	79
Nursing Homes	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Office of the Premier/Alberta Executive Council	0	0	0	0	0	0	0	0	0	0	16	1	0	0	0	0	17
Officers of the Legislature	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2
Panels	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Provincial Health Board (Health Quality Council)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Regional Health Authorities (Alberta Health Services)	0	0	5	0	0	3	0	0	1	2	35	4	0	1	0	0	51
School Districts	0	0	5	0	0	1	0	0	0	1	3	0	0	7	0	0	17
Universities	0	0	4	0	0	1	0	0	0	2	12	1	2	2	0	0	24
Other	0	0	0	0	0	1	0	0	1	2	7	0	0	1	0	0	12
Total	**1**	**0**	**91**	**4**	**2**	**33**	**5**	**0**	**14**	**26**	**303**	**26**	**81**	**22**	**1**	**1**	**610**

Note: The statistics do not include intake cases.

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period April 1, 2013 to March 31, 2014

HIA

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors/Physician Office System Program, Consultants)	0	0	0	0	0	0	3	0	0	3	0	0	0	6
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians	0	0	0	0	0	0	0	0	0	2	0	0	1	3
Chiropractors	0	0	0	0	0	0	1	0	24	0	0	0	0	25
Government Ministries/Departments	0	0	2	0	0	0	1	0	12	3	1	0	0	19
Minister of Health	0	0	0	0	0	0	1	0	0	0	0	0	0	1
Hospital Board (Covenant Health)	0	0	1	0	0	0	2	0	4	1	2	0	1	11
Dental Hygienists	0	0	0	0	0	0	0	0	2	0	0	0	0	2
Dentists	0	0	2	0	0	0	0	0	0	0	0	0	0	2
Denturists	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Health Professional Colleges and Associations	0	0	0	0	0	0	0	0	0	4	0	0	1	5
Long Term Care Centres	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Midwives	0	0	0	0	0	0	0	0	16	0	0	0	0	16
Nursing Homes	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Opticians	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Pharmacies/Pharmacists	0	0	2	0	0	0	1	0	49	0	0	0	2	54
Physicians	0	0	26	0	0	0	3	0	176	7	8	0	31	251
Primary Care Networks	0	0	0	0	0	0	0	0	20	1	0	0	4	25
Provincial Health Board (Health Quality Council)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Registered Nurses	0	0	0	0	0	0	0	0	24	2	0	0	0	26
Regional Health Authorities (Alberta Health Services)	0	0	16	0	0	0	2	1	40	4	35	0	20	118
Researchers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Research Ethics Boards	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subsidiary Health Corporations	0	0	1	0	0	0	0	0	1	0	0	0	3	5
Universities/Faculties of Medicine	0	0	0	0	0	0	1	0	0	1	0	0	1	3
Other	0	0	0	0	0	0	0	3	1	3	0	0	3	10
Total	**0**	**0**	**50**	**0**	**0**	**0**	**15**	**4**	**369**	**33**	**46**	**0**	**68**	**585**

Note: The statistics do not include intake cases

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period April 1, 2013 to March 31, 2014

PIPA Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services	0	0	6	0	0	0	0	0	0	0	2	0	5	13
Admin & Support Services	0	0	0	0	0	0	0	0	0	0	1	0	2	3
Architectural	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Dealers in Automobiles	0	0	5	0	0	0	0	0	0	0	1	0	0	6
Child Day-Care Services	0	0	0	0	0	0	0	0	0	0	1	0	1	2
Collection Agencies	0	0	4	0	0	0	0	0	0	0	0	0	0	4
Construction	0	0	1	0	0	0	0	0	0	0	4	0	1	6
Credit Bureaus	0	0	1	0	0	0	0	0	0	0	0	0	1	2
Educational Services	0	0	3	0	0	0	0	0	0	0	1	0	2	6
Finance	0	0	2	0	0	0	0	0	0	0	3	0	19	24
Private Healthcare & Social Assistance	0	0	4	0	0	0	0	0	0	0	4	0	7	15
Information & Cultural Industries	0	0	5	0	0	0	1	0	0	1	2	0	4	13
Insurance Industry	0	0	5	0	0	0	1	0	0	0	6	0	13	24
Investigative & Security Services	0	0	0	0	0	0	0	0	0	0	2	0	0	2
Legal Services	0	0	3	0	0	0	0	0	0	0	7	0	0	10
Manufacturing	0	0	2	0	0	0	1	0	0	0	0	0	8	11
Medical & Diagnostic Laboratories	0	0	1	0	0	0	0	0	0	0	0	0	0	1
Mining, Oil & Gas	0	0	3	0	0	0	0	0	0	0	0	0	9	12
Motor Vehicle Parts & Accessories	0	0	0	0	0	0	1	0	0	0	0	0	0	1
Nursing Homes/Home Health Care	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Professional, Scientific & Technical	0	0	0	0	0	0	0	0	0	0	1	0	0	1
Public Administration	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Real Estate, Rental, Leasing	0	0	11	0	0	0	10	0	0	0	0	0	0	21
Retail	0	0	4	0	0	0	0	0	0	0	2	0	8	14
Trades/Contractors	0	0	2	0	0	0	0	0	0	0	2	0	0	4
Transportation	0	0	0	0	0	0	0	0	0	0	1	0	0	1
Utilities	0	0	2	0	0	0	0	0	0	0	0	0	0	2
Wholesale Trade	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Arts, Entertainment & Recreation	0	0	4	0	0	0	0	0	0	0	0	0	1	5
Other	0	0	7	0	0	0	1	0	1	1	12	0	13	35
Total	**0**	**0**	**75**	**0**	**0**	**0**	**14**	**0**	**1**	**3**	**52**	**0**	**96**	**241**

Note: The statistics do not include intake cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from the period April 1, 2013 to March 31, 2014

FOIP Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Disclosure to Commissioner	Request Authorization to Indirectly Collect	Total
Agencies	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	2
Boards	0	0	11	1	0	0	1	0	0	1	9	2	2	0	0	0	27
Child and Family Service Authorities	0	0	6	0	0	0	0	0	0	0	1	0	4	0	0	0	11
Colleges	0	0	29	0	0	0	1	0	0	0	5	0	0	1	0	0	36
Commissions	0	0	1	0	0	1	0	0	0	0	7	1	2	0	0	0	12
Committees	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Federal Departments	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Foundations	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Government Ministries/ Departments	1	0	8	1	0	0	1	0	8	13	94	9	71	2	1	1	210
Hospital Board (Covenant Health)	0	0	0	0	0	0	0	0	0	0	4	0	0	1	0	0	5
Law Enforcement Agencies	0	0	3	2	0	1	1	0	0	1	20	0	0	1	0	0	29
Legislative Assembly Offices	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Local Government Bodies	0	0	0	0	0	1	0	0	0	0	2	0	0	1	0	0	4
Long Term Care Centres	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Municipalities	0	1	9	0	0	7	0	0	3	1	50	11	9	2	0	0	93
Nursing Homes	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
Officers of the Legislature	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Panels	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Premier's Office	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	9
Provincial Health Board (Health Quality Council	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Regional Health Authorities (Alberta Health Services)	0	0	5	0	0	1	0	0	1	1	31	1	0	0	0	0	40
School Districts	0	0	3	0	0	1	0	0	0	0	7	0	0	8	0	0	19
Universities	0	0	2	0	0	0	1	0	0	2	9	1	2	3	0	0	20
Other	0	0	0	0	0	0	1	0	1	2	6	0	0	0	0	0	10
Total	**1**	**1**	**77**	**4**	**0**	**12**	**6**	**0**	**13**	**22**	**258**	**26**	**90**	**21**	**1**	**1**	**533**

Note: The statistics do not include intake cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from the period April 1, 2013 to March 31, 2014

HIA

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors/Physician Office System Program, Consultants)	0	0	0	0	0	0	0	0	0	2	0	0	0	2
Associations, Boards, Councils, Commissions, Committees, Panels, or Agencies created by Custodians	0	0	0	0	0	0	0	0	0	5	0	0	2	7
Chiropractors	0	0	0	0	0	0	1	0	21	0	0	0	1	23
Dentists	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Dental Hygienists	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hospital Board (Covenant Health)	0	0	0	0	0	0	2	0	2	0	1	0	1	6
Long Term Care Centres	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nursing Homes	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Opticians	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Pharmacies/Pharmacists	0	0	1	0	0	0	1	0	48	0	0	0	3	53
Physicians	0	0	5	0	0	0	3	0	183	6	4	0	14	215
Primary Care Networks	0	0	0	0	0	0	0	0	14	1	0	0	3	18
Provincial Government Departments	0	0	3	0	0	0	1	0	12	3	1	0	0	20
Provincial Health Boards	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Researchers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Registered Nurses	0	0	0	0	0	0	0	0	21	3	0	0	0	24
Regional Health Authorities (Alberta Health Services)	0	0	5	0	0	0	3	0	43	4	11	0	10	76
Research Ethics Boards	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subsidiary Health Coporations	0	0	1	0	0	0	0	0	0	0	0	0	3	4
Universities/Faculties of Medicine	0	0	0	0	0	0	0	0	0	1	0	0	1	2
Other	0	0	0	0	0	0	2	0	0	3	0	0	2	7
Total	**0**	**0**	**15**	**0**	**0**	**0**	**13**	**0**	**344**	**29**	**17**	**0**	**40**	**458**

Note: The statistics do not include intake cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from the period April 1, 2013 to March 31, 2014

PIPA

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Request Advanced Ruling	Total
Accommodation & Food Services	0	0	3	0	0	0	1	0	0	0	2	0	3	0	8
Admin & Support Services	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
Construction	0	0	0	0	0	0	0	0	0	0	2	0	2	0	4
Credit Bureaus	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Dealers in Automobiles	0	0	7	0	0	0	0	0	0	0	0	0	0	0	7
Educational Services	0	0	1	0	0	0	0	0	0	0	2	0	1	0	4
Finance	0	0	0	0	0	0	2	0	0	0	2	0	13	0	17
Private Healthcare & Social Assistance	0	0	3	0	0	0	0	0	0	2	4	0	7	0	16
Information & Cultural Industries	0	0	2	0	0	0	0	0	0	0	1	0	3	0	6
Insurance Industry	0	0	4	0	0	0	0	0	0	0	6	0	7	0	17
Legal Services	0	0	2	0	0	0	0	0	0	0	5	0	1	0	8
Manufacturing	0	0	0	0	0	0	0	0	0	0	0	0	6	0	6
Mining, Oil & Gas	0	0	3	0	0	0	0	0	0	1	3	0	3	0	10
Newspaper Publishing	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Professional, Scientific & Tech.	0	0	0	0	0	0	0	0	0	0	1	0	1	0	2
Public Administration	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Real Estate, Rental & Leasing	0	0	6	0	0	0	0	0	0	0	2	0	0	0	8
Retail	0	0	1	0	0	0	0	0	0	0	0	0	5	0	6
Transportation	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2
Utilities	0	0	1	0	0	0	0	0	0	0	1	0	1	0	3
Wholesale Trade	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Arts, Entertainment & Recreation	0	0	1	0	0	0	0	0	0	0	0	0	2	0	3
Other	0	0	14	0	0	0	1	0	0	4	6	0	10	0	35
Total	**0**	**0**	**50**	**0**	**0**	**0**	**4**	**0**	**0**	**7**	**41**	**0**	**66**	**0**	**168**

Note: The statistics do not include intake cases

Appendix C: Orders, Decisions and Public Investigation Reports Issued

Statistics are from the period April 1, 2013 to March 31, 2014

FOIP RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta Education	1	0	0	1
Alberta Energy	1	0	0	1
Alberta Environment and Sustainable Resource Development	1	0	0	1
Alberta Health	3	0	0	3
Alberta Health Services	3	0	0	3
Alberta Human Rights Commission	1	0	0	1
Alberta Human Services	1	0	0	1
Alberta Justice and Solicitor General	9	0	0	9
Alberta Treasury Branches	0	1	0	1
Bow Valley College	1	0	1	2
Calgary Board of Education	1	0	0	1
Calgary Police Service	1	0	0	1
Calgary Roman Catholic Separate School District #1	2	0	0	2
Central Alberta Child & Family Services Authority	1	0	0	1
City of Calgary	3	0	0	3
City of Camrose	1	0	0	1
City of Edmonton	3	0	0	3
City of Lethbridge	1	0	0	1
City of Red Deer	1	0	0	1
County of Vermilion River	1	0	0	1
Covenant Health	2	0	0	2
East Central Alberta Child & Family Services Authority	1	0	0	1

FOIP RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
Edmonton & Area Child & Family Services Authority	2	0	0	2
Edmonton Police Service	2	0	1	3
Energy Resources Conservation Board	1	0	0	1
Evergreen Waste Management Services Committee	1	0	0	1
Law Enforcement Review Board	0	0	1	1
Lethbridge College	1	0	0	1
Medicine Hat Police Service	1	0	0	1
Out-of-Country Health Services Committee	1	0	0	1
Out-of-Country Health Services Committee Appeal Panel	1	0	0	1
Pembina Hills Regional Division No. 7	1	0	0	1
Service Alberta	0	0	1	1
Southwest Alberta Child & Family Services Authority	1	0	0	1
Town of Ponoka	1	0	0	1
Town of Taber	1	0	0	1
University of Alberta	1	0	0	1
University of Calgary	2	0	0	2
Workers' Compensation Board	5	0	0	5
Sub-Total	**61**	**1**	**4**	**66**

HIA RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
*Alberta Health/Alberta Health Services	0	0	1	1
Alberta Health Services	1	0	-	1
Amani Pharmacy Ltd.	0	0	1	1
Covenant Health	1	0	0	1
Dr. Ashif Jaffer	0	0	1	1
Dr. Dianne Smith	0	0	1	1
Dr. Nagy Youssef	1	0	0	1
Sub-Total	**3**	**0**	**4**	**7**

PIPA RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta Treasury Branches	0	0	1	1
ATCO Electric Ltd. & Canadian Utilities Ltd.	1	0	0	1
Contour Earthmoving Ltd.	1	0	0	1
Moore's Industrial Service Ltd.	1	0	0	1
Professional Drivers Bureau of Canada	1	0	0	1
Project Porchlight	1	0	0	1
Sangha Operating Group Inc.	1	0	0	1
Sobeys Group Inc.	1	0	0	1
Suncor Energy Inc.	1	0	0	1
TD Insurance	1	0	0	1
The Legal Aid Society of Alberta	1	0	0	1
Sub-Total	**10**	**0**	**1**	**11**
Total	**74**	**1**	**9**	**84**

* H2013-IR-02 had both Alberta Health and Alberta Health Services as respondent custodians.

FOIP Orders: 61 (70 cases)
FOIP Decisions: 1 (1 case)
FOIP Investigation Reports: 4 (32 cases)
HIA Orders: 3 (3 cases)
HIA Decisions: 0
HIA Investigation Reports: 4 (5 cases)
PIPA Orders: 10 (10 cases)
PIPA Decisions: 0
PIPA Investigation Reports: 1(1 cases)

* A single Order, Decision or Investigation Report can relate to more than one entity and more than one file.

The number of Orders, Decisions and Investigation Reports are counted by the number of Order, Decision or Investigation Report numbers assigned.

Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released. Investigation Reports are recorded by the date they were publicly issued.

A copy of all Orders, Decisions and Investigation Reports are available on the OIPC web site www.oipc.ab.ca.

Appendix D: Accepted Privacy Impact Assessments by Public Body and Custodian Types

Statistics are from the period April 1, 2013 - March 31, 2014

PUBLIC BODY	PIA TITLE
MINISTRIES/DEPARTMENTS	
Alberta Health	Alberta Health and Privacy Office Redaction (ATIPXpress) Software
	Alberta Seniors Property Tax Deferral (SPTD) Program
	Service Alberta (SA) Special Investigations Unit (SIU) - Fraud and Compliance Investigations
Alberta Human Services	Part A; Compliance Mangement Information Systems (CMIS) PIA
Alberta Innovation and Advanced Education	Alberta Immigrant Nominee Program (AINP)
Service Alberta	Public Disclosure of Travel and Expenses
	Legal Name Change Publication Procedure
OTHER PUBLIC BODIES	
Alberta Innovates - Health Solutions	Provincial Health Research Ethics Information System
MUNICIPALITIES	
City of Cold Lake	City of Cold Lake Surveillance Cameras Located in Public Areas
	1. Cold Lake RegionalAerodrome - CEN 5 Surveillance Cameras 2. City of Cold Lakes' Public Works Shop Surveillance Cameras 3. City's Transfer Station and Class III Landfill Surveillance Cameras
Strathcona County	When to Work Software Project
REGIONAL HEALTH AUTHORITIES	
Alberta Health Services	Human Resource Management System (HRMS) Project - ePeople

CUSTODIAN	PIA TITLE
CHIROPRACTORS	
Dr. Tyler Fix	ChiroSUITE
Dr. (Kerry) Joelle Johnson	Implementation of ChiroSUITE v5 Electronic Patient Record System
Dr. Bradley William Kane	ChiroTouch
Dr. Bretton R. Baynes	ChiroSUITE V5
Dr. Brian Rapcewicz	Progressive Wellness Centre
Dr. Candice Hueppelsheuser	ChiroSUITE V5
Dr. Corissa Audren	Electronic Medical Records (EMR) to: ATLAS Chiropractic System
Dr. Derek Lampshire	Medical Records (EMR)
Dr. Gord McMorland	ChiroSUITE v5 Electronic Patient Record System
Dr. Jacqueline Boyd	Medical Records (EMR) to: ATLAS Chiropractic System
Dr. Jamila Abdulla	Billing, Patient Scheduling, Patient Tracking and Chart Notes
Dr. Jeff Warren	Medical Records (EMR)
Dr. John Scott	Atlas Electronic Medical Record
Dr. Kevin Aitken	Edge Chiropractic & Sport Therapy Electronic Medical Record Project
Dr. Melanie Beingessner	ChiroSUITE
Dr. Neetash Patel	Medical Records (EMR)
Dr. Nicole Fox	Implementation of ChiroSUITE v5 Electronic Patient Record System
Dr. Ryan Wagemakers	ChiroSUITE V5

CUSTODIAN	PIA TITLE
HOSPITAL BOARD	
Covenant Health	CBORD Nutrition Service Suite
	Amendment to the Centricity Perinatal (CPN) System
MINISTRY HIA	
Alberta Health	Immunization/Adverse Reaction to Immunization (Imm/ADI) Addendum #5
	Addendum 1: Health Human Resource Forecasting and Simulation Model (HFSM) - Name Change to Health Workforce Forecasting Mode (HWFM) and Update to Data Listing
	Addendum 1: National Physician Database (NPDB) - Additional Data for Feasibility Analysis
	Addendum 2 - New Temporary Neighborhoods
	Addendum 3: Alberta Continuing Care Information System (ACCIS) - Updates to Data Listing and Data Extracts to CIHI.
	Alberta Cancer Registry (ACR) Addendum 1 - ACR Data Sharing and Interim Access Process
	Business Intelligence Environment (BIE) PIA Addendum 6
	First Addendum to the Newborn Metabolic Screening
	Pilot Family Care Clinic (FCC) Data
	Public Health and Surveillance Privacy Impact Assessment Addendum 3 - Ticks
	Public Health Surveillance
PHARMACIES/PHARMACISTS	
	44 Alberta Netcare PIAs
Loblaw Companies Limited - H	Pharmacy Central Reporting
Shoppers Drug Mart 2413	Pharmacy Immunization Program
Sobeys Inc. Pharmacy	PIA Amendment H3441
Winter's Pharmacy/ Winter's Pharmacy North	Winter's Pharmacy and Winter's Pharmacy North Pharmacy Immunization Program

CUSTODIAN	PIA TITLE
PHYSICIANS	
	77 Physician Office System Program (POSP) PIAs
	52 Alberta Netcare PIAs
Dr. Ali Abdullah	Mediplan of Telin Electronic Medical Records (EMR)
Dr. Christopher Lever	Amendment - Email Services
Dr. H. Potgieter	Organization Management and inclusion in the Kalyna Country PCN
Dr. Jennifer Norheim	Teen Health Clinic
Dr. Michael Poitras	Edmonton West PCN, Organizational Privacy Management, Primary Care Team Program, Specialized Referral Coordination
Dr. Robert Chan	EMR with Optimed
Dr. Robert J. Bailey	Outsources Transcription Services
Dr. Sandy Tam	Accuro Pro EMR System
Dr. Shona Imlah	ACCRO Electronic Medical Record
Dr. Wendi Kisic	Chirosoft
Dr. Alykhan Nanji	Increased Services Offered by Nanji PC Clinics (C-era, C-endo, C-o2)
Dr. Amber Whitford	Non-POSP PIA, Nightingale Informatix
Dr. Barrie Steed	PACS System
Dr. Bruce Taylor (inactive, see Dr. Tom Yeo)	MICConnect
Dr. Cathy Copeland	Transmission of Diagnostic Imaging Test Reports to Alberta Health Services
Dr. Chris Siwak	Amendment to the Alberta Health Services Diagnostic Imagining and Text Repository
Dr. Christopher Gee	Amendment - Wireless Network
Dr. Dorcas Kennedy	Amendment: Implementation of wireless network capability
Dr. Fawzi Mabruk Fetouri	Microquest Healthquest EMR
Dr. Francois Bolduc	Fragile X Syndrome Patient Registry
Dr. Harshi Mathur	Electronic Medical Records (EMR)

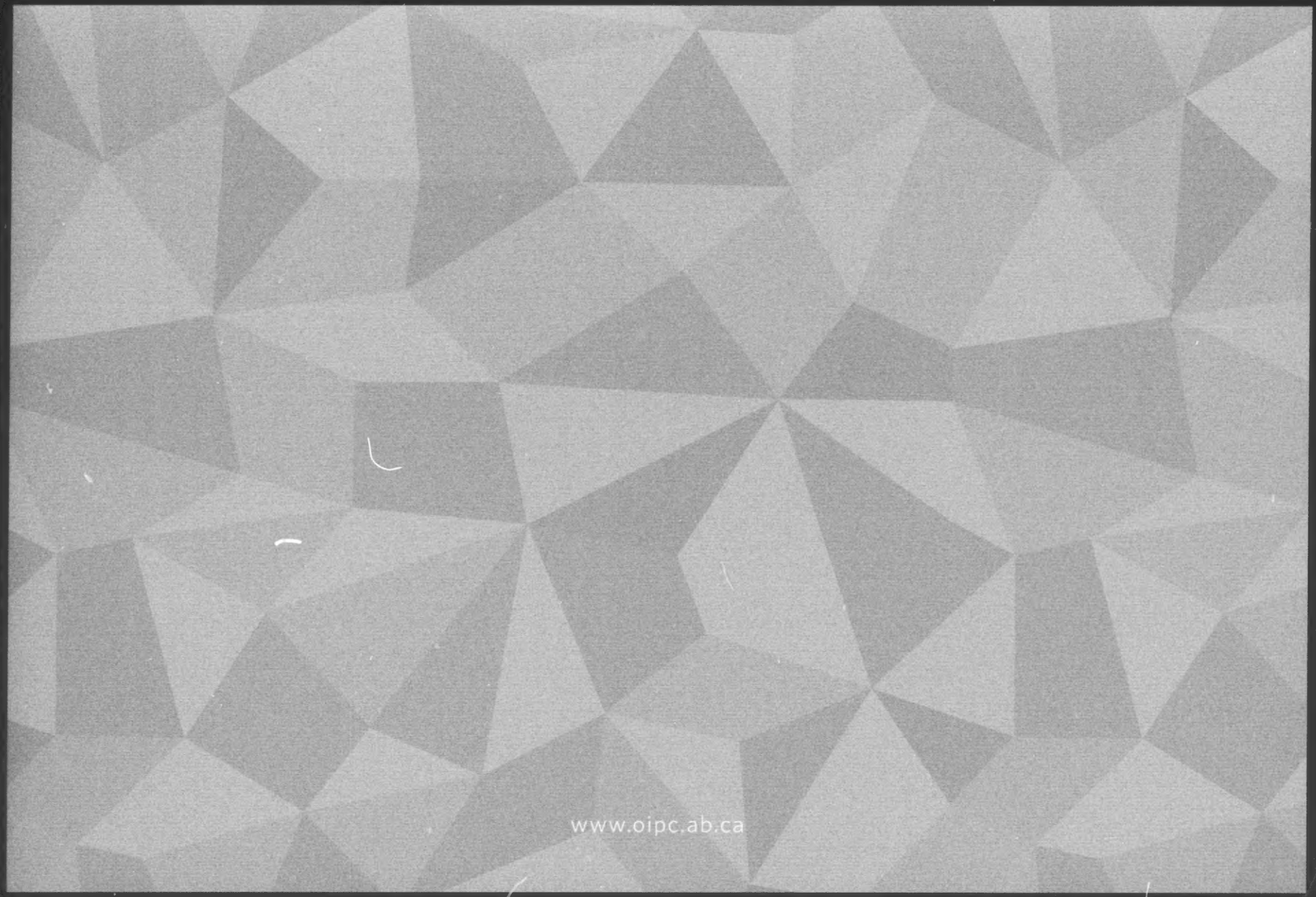
CUSTODIAN	PIA TITLE
Dr. Hien Huynh	Pediatric Inflammatory Bowel Disease Patient Registry
Dr. I. Gardiner	Addendum; Integration with the Alberta DI Repository
Dr. J. Peter Giannoccaro	Amendment: Sending RACPC Reports to Netcare
Dr. Jennifer Walker	University of Alberta Wellness Alert Disease Surveillance Program in Residence
Dr. Jennifer Adams-Hessel	Northwest Wellness Centre, Grimshaw Chiropractic Care Centre and Sharing Information with the Grande Prairie Primary Care Network
Dr. Kevin Govender	Amendment to H5679 - Inclusion of staff from Lloydminster PCN access to custodian's EMR to expedited referral process
Dr. Laura Cano	Optimed ASP Hosted EMR Solution.
Dr. Lofti Seysan	Intele RIS EMR /RIS/EMB Pacs Implementation
Dr. Michael Coe	Diagnostic Images to Alberta Health Services' Data Repository
Dr. Neeraj Bector	MD DataBank's eHealth Vault Implementation
Dr. Neil S. Brass	Outsourced Transcription and Outsourced Billing Agent
Dr. Piush Mandhane	Pediatric Respiratory Medicine Program Patient Registry
Dr. Raymond Lai	Kiestra Microbiology Total Lab Automation
Dr. Reyhana Ahmed	Outsourced Transcription and Outsourced Billing Agen
Dr. Ryan A. Carter	Move from paper record to EMR
Dr. Sarah Koles	Amendment to Radiology Information System/Picture Archiving and Communications System ASP Project - H0991
Dr. Stephanie Dotchin	Management and Organization Information Management
Dr. Stephen R. Fugler	Outsourced Transcription and Outsourced Billing Agent
Dr. Trevor Chan	Electronic Billing Application
Dr. Wing Lim	Telus Health Solutions Wolf ASP hosted EMR
Canada Diagnostic Centres	Amendment to Canada Diagnostic Centres' Patient Imaging System (PACS & RIS)

CUSTODIAN	PIA TITLE
REGISTERED NURSES	
	3 Alberta Netcare PIAs
Mr. Duncan Bray	Paper community health records to an Electronic Community Health and Immunization Program (CHIP), Paper diabetes management records to an electronic Diabetes Community Assessment, Response and Evaluation (CARE) Solution
	Practice Solutions Suite EMR Implementation ASP Model to Alberta Netcare
Ms. Alexis Legall	Community Health Information Systems
Ms. Elizabeth Alix McGregor	Community Health and Immunization Program (CHIP), Community Assessment Response and Empowerment (CARE)
Ms. Helen Littlechild	Community Health Information System
Ms. Dorothy Janetzki	Health Services Electronic Community Health Information System - Community Health and Immunization Program (CHIP)
Ms. Gloria Fraser	Bigstone Health Commission Homecare Reporting System
	Health System Project
Ms. Jane Marston	Management and Organization Information Management and Netcare Access
Ms. Karen Benwell	MHC and BHC Electronic Community Health Information System
	North Peace Tribal Council Homecare Reporting System
Ms. Laura Tomkins	Community Health Information System
	Sucker Creek First Nation Health Centre Electronic Home Care Reporting System Project
Ms. Liz Waker	Tsuu T'ina Health and Wellness Centre Electronic Community Health Information System
Mr. Dave Bateman	Organization Management and Organization Information Management and Alberta Netcare
Ms. Mary Flondra	Goodfish Lake Health Centre Electronic Health
Ms. Sandra Livingston	O'Chiese Health Centre Electronic Community Health Information system - Community Health and Immunization Program (CHIP)
Ms. Susan McGillis	Enoch Cree Nation Health Services Home Care Reporting System
Ms. Susan Stoneson	Community Health and Immunization Program (CHIP), Community Assessment Response and Empowerment (CARE)

CUSTODIAN	PIA TITLE
REGIONAL HEALTH AUTHORITIES	
Alberta Health Services	Consolidated Laboratory Data Repository (CLDR)
	Data Integration for Alberta Laboratories (DIAL)
	eCritical System - Clinical (MetaVision)
	Provincial CBORD
	Alberta Bone & Joint Replacement Operating Room Reporting System
	Alberta Health Services Client Registry (CR)
	Amendment to Enterprise Business Intelligence (EBI) Program
	Amendment to the CBORD
	Anatomic Pathology (AP) Specimen Tracking
	BDM Pharmacy System - Calgary Zone
	Calgary Firefighters' Burn Treatment Centre Burn Registry
	Cancer in Youth Canada (CYP-C)
	Cancer Surgery Alberta - Synpotec System
	CareLink Remote Monitoring System
	Chronic Disease Management Quality of Life Measurement Tool
	Chronic Obstructive Pulmonary Disease Self Initiative (CSI) Database
	Community Care Local Database PIA -Amendment #5
	Corrections Health Services - Health Record Amendment #1
	Data Warehouse (ICU Tracer)
	e-CLINICIAN Project Enterprise Privacy Impact Assessment
	EMS Community Paramedic Program - Calgary Zone
	Environmental Public Health (EPH) Provincial Implementation of Hedgehog Environmental Reporting System PIA
	eReferral Management System

CUSTODIAN	PIA TITLE
	Feedback and Concerns Tracking (FACT)
	Gastroenterology Services (Calgary) EndoPRO PIA.
	Human Resource Management System (HRMS) Project - ePeople
	Identity and Access Management (IAM) - Alberta Netcare Phase 2
	iPHIS Provincial TB Information System
	Maternal Fetal Medicine - Astraia Implementation
	MEDITECH Integrated Health Information Management Complex
	MEDITECH Integrated Health Information Management Complex PIA Amendment #1 - Case Manager Information to Netcare
	Medworxx Utilization Management System (UMS) - Provincial
	Netcare Clinical Repositories (NCR) PIA Addendum
	nSight Pulmonary Diagnostics
	Picture Archiving Communication System (PACS) for the former Northern Lights Health Region (NLHR)
	Procure-to-Pay (P2P) Project
	Provincial Diagnostic Imaging (DI) Picture Archiving and Communication System (PACS) PIA
	Provincial Telehealth
	ProvSurv Amendment #2
	Pulmonary Function Testing Patient Data Repository (PFTPDR) to Netcare
	Reporting and Learning System (RLS)
	Sexually Transmitted Infections (STI) Centralized Services Database.
	Transition of Alberta Aids to Daily Living Respiratory Benefits Program from Alberta Health to Alberta Health Services.

CUSTODIAN	PIA TITLE
PRIMARY CARE NETWORKS	
	*Note PCN PIAs Involving POSP EMR implementation or Alberta Netcare Implementation have already been accounted for in the "Physician" section of this table.
Edmonton North Primary Care Network	Specialist Referral Database
Leduc Beaumont Devon Primary Care Network	Appointment Reminders
	Connected Wellness Platform Application
	Prescription to Get Active Program
Palliser Primary Care Network	Data Matching PIA
Red Deer Primary Care Network	Amendment to the Red Deer PCN Portal Project
	Information Privacy and Security Policies
Sherwood Park - Strathcona County Primary Care Network	Sherwook Park Remote Patient Monitoring Pilot Project
	Virtual Care Management Pilot
Wolf Creek Primary Care Network (PCN)	Evaluation Data Collection Methods


www.oipc.ab.ca